Wind River LinuxSecurity Bulletin - 2020-04-10

Wind River has analyzed the following security alerts and determined the status to be as shown for each with respect to Wind River Linux. Visit *http://cve.mitre.org/* for more information on these security alerts. For issues still under investigation, if it is determined a vulnerability exists, a patch will be made available and notification sent via Wind River Online Support (OLS). Visit *http://www.windriver.com/support/* and click on the link to "Access Online Support" to download a patch.

Index:

Table A: All CVEs Modified or Added this Report
Table B: All Analyzed CVEs Affecting or Potentially Affecting WRLinux
Table C: All Analyzed CVEs

8.0.0.28 release; Not vulnerable = eatch releases are:

WRLinux 8.0.0.30
WRLinux 9.0.0.21
WRLinux LTS 17 10.17.41.16
WRLinux LTS 18

Table A: All CVEs Modified or Added this Report

CVE Number	Priority	CVSSv3_Severity	CVE Description	WR Comments	Modifications	Status WRLinux 8.0.0	Status WRLinux 9.0.0	Status WRLinux LTS 17	Status WRLinux LTS 18	Status WRLinux LTS 19	Status WRLinux CD release	Defect
CVE-2020-9383	LOW	HIGH	An issue was discovered in the Linux kernel through 5.5.6. set_fdc in drivers/block/floppy.c leads to a wait_til_ready out-of-bounds read because the FDC index is not checked for errors before assigning it, aka CID-2e90ca68b0d2.	linux	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.7	Not vulnerable	LIN1019-4079
CVE-2020-8835	HIGH	HIGH	In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780)	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Vulnerable	Not vulnerable	LIN1019-4231
CVE-2020-8834			KVM in the Linux kernel on Power8 processors has a conflicting use of HSTATE_HOST_R1 to store r1 state in kvmppc_hv_entry plus in kvmppc_{save,restore}_tm, leading to a stack corruption. Because of this, an attacker with the ability run code in kernel space of a guest VM can cause the host kernel to panic. There were two commits that, according to the reporter, introduced the vulnerability: f024ee098476 (KVM: PPC: Book3S HV: Pull out TM state save/restore into separate procedures) 87a11bb6a7f7 (KVM: PPC: Book3S HV: Work around XER[SO] bug in fake suspend mode) The former landed in 4.8, the latter in 4.17. This was fixed without realizing the impact in 4.18 with the following three commits, though it's believed the first is the only strictly necessary commit: 6f597c6b63b6 (KVM: PPC: Book3S PR: Add guest MSR parameter for kvmppc_save_tm()/kvmppc_restore_tm()) 7b0e827c6970 (KVM: PPC: Book3S HV: Factor fake-suspend handling out of kvmppc_save/restore_tm) 009c872a8bc4 (KVM: PPC: Book3S PR: Move kvmppc_save_tm/kvmppc_restore_tm to separate file)	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4268
CVE-2020-8832			The fix for the Linux kernel in Ubuntu 18.04 LTS for CVE-2019-14615 (The Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors.) was discovered to be incomplete, meaning that in versions of the kernel before 4.15.0-91.92, an attacker could use this vulnerability to expose sensitive information.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4270
CVE-2020-8649	LOW	HIGH	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vgacon_invert_region function in drivers/video/console/vgacon.c.	linux	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.16	10.19.45.7	Investigate	LIN1019-4010
CVE-2020-8648	LOW	HIGH	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.	linux	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.7	Investigate	LIN1019-4011
CVE-2020-8552	MEDIUM	HIGH	The Kubernetes API server component in versions prior to 1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via successful API requests.	kubernetes	Updated	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Investigate	Investigate	LIN1019-4189
CVE-2020-8551	LOW	MEDIUM	The Kubelet component in versions 1.15.0-1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via the kubelet API, including the unauthenticated HTTP read-only API typically served on port 10255, and the authenticated HTTPS API typically served on port 10250.	kubernetes	Updated	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Investigate	Investigate	LIN1019-4190
CVE-2020-8428	LOW	HIGH	fs/namei.c in the Linux kernel before 5.5 has a may_create_in_sticky use-after-free, which allows local users to cause a denial of service (OOPS) or possibly obtain sensitive information from kernel memory, aka CID-d0cb50185ae9. One attack vector may be an open system call for a UNIX domain socket, if the socket is being moved to a new parent directory and its old parent directory is being removed.	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.7	Not vulnerable	LIN1019-3978
CVE-2020-7066	MEDIUM	MEDIUM	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using get_headers() with user-supplied URL, if the URL contains zero (\0) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.	php	Updated	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.16	10.19.45.7	Investigate	LIN1019-4208
CVE-2020-7065	MEDIUM	HIGH	In PHP versions 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using mb_strtolower() function with UTF-32LE encoding, certain invalid strings could cause PHP to overwrite stack-allocated buffer. This could lead to memory corruption, crashes and potentially code execution.	php	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.7	Investigate	LIN1019-4209
CVE-2020-7064	MEDIUM	MEDIUM	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.	php	Updated	8.0.0.33	9.0.0.25	10.17.41.21	10.18.44.16	10.19.45.7	Investigate	LIN1019-4210

	A	B	C	D	E	F	G	H	I	J	K	L	M
25	CVE-2020-6096	HIGH	CRITICAL	An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.	glibc	Updated	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4216
26	CVE-2020-5504	MEDIUM	HIGH	In phpMyAdmin 4 before 4.9.4 and 5 before 5.0.1, SQL injection exists in the user accounts page. A malicious user could inject custom SQL in place of their own username when creating queries to this page. An attacker must have a valid MySQL account to access the server.	phpmyadmin	Updated	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3909
27	CVE-2020-1934	HIGH	CRITICAL	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.	apache2	Updated	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4217
28	CVE-2020-1747	HIGH	CRITICAL	A vulnerability was discovered in the PyYAML library in versions before 5.3.1, where it is susceptible to arbitrary code execution when it processes untrusted YAML files through the full_load method or with the FullLoader loader. Applications that use the library to process untrusted input may be vulnerable to this flaw. An attacker could use this flaw to execute arbitrary code on the system by abusing the python/object/new constructor.	python-pyyaml	Updated	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4178
29	CVE-2020-1712			A heap use-after-free vulnerability was found in systemd before version v245-rc1, where asynchronous Polkit queries are performed while handling dbus messages. A local unprivileged attacker can abuse this flaw to crash systemd services or potentially execute code and elevate their privileges, by sending specially crafted dbus messages.	systemd	Updated	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1019-4212
30	CVE-2020-11668			In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4269
31	CVE-2020-11656			In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement.	sqlite3	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4261
32	CVE-2020-11655			SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the AggInfo object's initialization is mishandled.	sqlite3	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4262
33	CVE-2020-11609	MEDIUM	MEDIUM	An issue was discovered in the stv06xx subsystem in the Linux kernel before 5.6.1. drivers/media/usb/gspca/stv06xx/stv06xx.c and drivers/media/usb/gspca/stv06xx/stv06xx_pb0100.c mishandle invalid descriptors, as demonstrated by a NULL pointer dereference, aka CID-48fe96eadb93.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4253
34	CVE-2020-11608	LOW	MEDIUM	An issue was discovered in the Linux kernel before 5.6.1. drivers/media/usb/gspca/ov519.c allows NULL pointer dereferences in ov511_mode_init_regs and ov518_mode_init_regs when there are zero endpoints, aka CID-998912346c0d.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4254
35	CVE-2020-11565	MEDIUM	HIGH	An issue was discovered in the Linux kernel through 5.6.2. mpol_parse_str in mm/mempolicy.c has a stack-based out-of-bounds write because an empty nodelist is mishandled during mount option parsing, aka CID-aa9f7d5172fa.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4245
36	CVE-2020-11501	MEDIUM	CRITICAL	GnuTLS 3.6.x before 3.6.13 uses incorrect cryptography for DTLS. The earliest affected version is 3.6.3 (2018-07-16) because of an error in a 2017-10-06 commit. The DTLS client always uses 32 '\0' bytes instead of a random value, and thus contributes no randomness to a DTLS negotiation. This breaks the security guarantees of the DTLS protocol.	gnutls	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4237
37	CVE-2020-11494	LOW	MEDIUM	An issue was discovered in slc_bump in drivers/net/can/slcan.c in the Linux kernel through 5.6.2. It allows attackers to read uninitialized can_frame data, potentially containing sensitive information from kernel stack memory, if the configuration lacks CONFIG_INIT_STACK_ALL, aka CID-b9258a2cece4.	linux	Updated	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1019-4230
38	CVE-2020-11102	HIGH	CRITICAL	hw/net/tulip.c in QEMU 4.2.0 has a buffer overflow during the copying of tx/rx buffers because the frame size is not validated against the r/w data length.	qemu	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4249
39	CVE-2020-10942	MEDIUM	MEDIUM	In the Linux kernel before 5.5.8, get_raw_socket in drivers/vhost/net.c lacks validation of an sk_family field, which might allow attackers to trigger kernel stack corruption via crafted system calls.	linux	Updated	8.0.0.33	9.0.0.25	Investigate	10.18.44.16	Investigate	10.20.15.0	LIN1019-4176
40	CVE-2020-10941	MEDIUM	MEDIUM	Arm Mbed TLS before 2.6.15 allows attackers to obtain sensitive information (an RSA private key) by measuring cache usage during an import.	mbedtls	Updated	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4177
41	CVE-2020-10804	MEDIUM	HIGH	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability was found in retrieval of the current username (in libraries/classes/Server/Privileges.php and libraries/classes/UserPassword.php). A malicious user with access to the server could create a crafted username, and then trick the victim into performing specific actions with that user account (such as editing its privileges).	phpmyadmin	Updated	Investigate	Investigate	Investigate	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4157
42	CVE-2020-10803	LOW	MEDIUM	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability was discovered where malicious code could be used to trigger an XSS attack through retrieving and displaying results (in tbl_get_field.php and libraries/classes/Display/Results.php). The attacker must be able to insert crafted data into certain database tables, which when retrieved (for instance, through the Browse tab) can trigger the XSS attack.	phpmyadmin	Updated	Investigate	Investigate	Investigate	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4164

	A	B	C	D	E	F	G	H	I	J	K	L	M
43	CVE-2020-10802	MEDIUM	HIGH	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability has been discovered where certain parameters are not properly escaped when generating certain queries for search actions in libraries/classes/Controllers/Table/TableSearchController.php. An attacker can generate a crafted database or table name. The attack can be performed if a user attempts certain search operations on the malicious database or table.	phpmyadmin	Updated	Investigate	Investigate	Investigate	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4165
44	CVE-2020-10593	MEDIUM	HIGH	Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows remote attackers to cause a Denial of Service (memory leak), aka TROVE-2020-004. This occurs in circpad_setup_machine_on_circ because a circuit-padding machine can be negotiated twice on the same circuit.	tor	Updated	Not vulnerable	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-7115
45	CVE-2020-10592	MEDIUM	HIGH	Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows remote attackers to cause a Denial of Service (CPU consumption), aka TROVE-2020-002.	tor	Updated	Not vulnerable	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-7114
46	CVE-2019-9924	HIGH	HIGH	rbash in Bash before 4.4-beta2 did not prevent the shell user from modifying BASH_CMDS, thus allowing the user to execute any command with the permissions of the shell.	bash	Updated	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3770
47	CVE-2019-20636	HIGH	CRITICAL	In the Linux kernel before 5.4.12, drivers/input/input.c has out-of-bounds writes via a crafted keycode table, as demonstrated by input_set_keycode, aka CID-cb222aed03d7.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4263
48	CVE-2019-20054	MEDIUM	MEDIUM	In the Linux kernel before 5.0.6, there is a NULL pointer dereference in drop_sysctl_table() in fs/proc/proc_sysctl.c, related to put_links, aka CID-23da9588037e.	linux	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN1019-3872
49	CVE-2019-19769	MEDIUM	HIGH	In the Linux kernel 5.3.10, there is a use-after-free (read) in the perf_trace_lock_acquire function (related to include/trace/events/lock.h).	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.7	Not vulnerable	LIN1019-3775
50	CVE-2019-18860	MEDIUM	MEDIUM	Squid before 4.9, when certain web browsers are used, mishandles HTML in the host (aka hostname) parameter to cachemgr.cgi.	squid	Updated	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4158
51	CVE-2019-15167			Tcpdump is vulnerable to a buffer overflow, caused by improper bounds checking by the lmp_print_data_link_subobjs function in print-lmp.c. By sending specially-crafted data, a remote attacker could overflow a buffer and cause the application to crash.	tcpdump	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN1019-4137
52	CVE-2019-14615	LOW	MEDIUM	Insufficient control flow in certain data structures for some Intel(R) Processors with Intel(R) Processor Graphics may allow an unauthenticated user to potentially enable information disclosure via local access.	linux	Updated	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4267
53	CVE-2019-13627	Medium	HIGH	It was discovered that there was a ECDSA timing attack in the libgcrypt20 cryptographic library. Version affected: 1.8.4-5, 1.7.6-2+deb9u3, and 1.6.3-2+deb8u4. Versions fixed: 1.8.5-2 and 1.6.3-2+deb8u7.	libgcrypt	Updated	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	10.19.45.6	10.20.15.0	LIN1018-5046
54	CVE-2019-11254	MEDIUM	MEDIUM	The Kubernetes API Server component in versions 1.1-1.14, and versions prior to 1.15.10, 1.16.7 and 1.17.3 allows an authorized user who sends malicious YAML payloads to cause the kube-apiserver to consume excessive CPU cycles while parsing YAML.	kubernetes	Updated	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Investigate	Investigate	LIN1019-4220
55	CVE-2019-11251	MEDIUM	MEDIUM	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	kubernetes	Updated	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	10.19.45.5	10.20.15.0	LIN1019-4047
56	CVE-2018-8086			The basename implementation in string/basename.c in the GNU C Library (aka glibc or libc6) 2.26 allows attackers to cause a denial of service (segmentation fault), within the assembly code for strrchr, via a crafted argument.	glibc	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3582
57	CVE-2018-4700			A flaw was found in the CUPS printing server. Insufficient randomness makes session cookies predictable, breaking CSRF protection.	cups	Updated	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3303
58	CVE-2018-20796	Medium	HIGH	In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227])(\\1\\1|t1|\\2537)+' in grep.	glibc	Updated	None	None	None	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3784
59	CVE-2018-19325	MEDIUM	HIGH	tcpdump 4.9.2 (and probably lower versions) is prone to a heap-based buffer over-read in the EXTRACT_32BITS function (extract.h, called from the rx_cache_find function, print-rx.c) due to improper serviceId sanitization.	tcpdump	Updated	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1019-4149
60	CVE-2018-14553	MEDIUM	HIGH	gdImageClone in gd.c in libgd 2.1.0-rc2 through 2.2.5 has a NULL pointer dereference allowing attackers to crash an application via a specific function call sequence. Only affects PHP when linked with an external libgd (not bundled).	gd	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.5	Not vulnerable	LIN1019-4035
61	CVE-2018-14378			An issue was discovered in LibTIFF 4.0.9. A buffer overflow can occur via an invalid or empty tif argument to TIFFWriteBufferSetup in tif_write.c, and it can be exploited (at a minimum) via the following high-level library API function: TIFFWriteTile.	tiff	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4396
62	CVE-2018-14375			An issue was discovered in LibTIFF 4.0.9. A buffer overflow vulnerability can occur via an invalid or empty tif argument to TIFFRGBAImageOK in tif_getimage.c, and it can be exploited (at a minimum) via the following high-level library API functions: TIFFReadRGBAImage, TIFFRGBAImageOK, and TIFFRGBAImageBegin.	tiff	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4412
63	CVE-2018-14374			An issue was discovered in LibTIFF 4.0.9. A buffer overflow can occur via an empty fmt argument to unixErrorHandler in tif_unix.c, and it can be exploited (at a minimum) via the following high-level library API functions: TIFFClientOpen, TIFFFdOpen, TIFFRawStripSize, TIFFCheckTile, TIFFComputeStrip, TIFFReadRawTile, TIFFUnRegisterCODEC, and TIFFWriteEncodedTile.	tiff	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4370

	A	B	C	D	E	F	G	H	I	J	K	L	M
64	CVE-2018-14373			An issue was discovered in LibTIFF 4.0.9. In TIFFFindField in tif_dirinfo.c, the structure tif is being dereferenced without first checking that the structure is not empty and has the requested fields (tif_foundfield). In the call sequences following from the affected library functions (TIFFVGetField, TIFFVGetFieldDefaulted, TIFFVStripSize, TIFFScanlineSize, TIFFTileSize, TIFFGetFieldDefaulted, and TIFFGetField), this sanitization of the tif structure is never being done and, hence, using them with an invalid or empty tif structure will trigger a buffer overflow, leading to a crash.	tiff	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4449
65	CVE-2018-12422	HIGH	CRITICAL	** DISPUTED ** addressbook/backends/ldap/e-book-backend-ldap.c in Evolution-Data-Server in GNOME Evolution through 3.29.2 might allow attackers to trigger a Buffer Overflow via a long query that is processed by the strcat function. NOTE: the software maintainer disputes this because the code had computed the required string length first, and then allocated a large-enough buffer on the heap.	evolution-data-server	Updated	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Won't Fix	LIN1019-3674
66	CVE-2018-10195			Lrzsz has an integer overflow vulernability in the src/zm.c:zsdata() function. An attacker could exploit this with the sz command to cause a crash or potentially leak information to the receiving server.	lrzsz	Updated	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4857
67	CVE-2018-1000845			Avahi version 0.7 contains a Incorrect Access Control vulnerability in avahi-daemon that can result in Traffic reflection and amplification for DDoS attacks.. This attack appear to be exploitable via unicast IP network packet with spoofed source address.	avahi	Updated	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3341
68	CVE-2017-7516			It was found that the cpio --no-absolute-filenames option since version 2.7 did not verify paths during extraction. A specially crafted cpio archive could bypass this option and write to an arbitrary location, outside of the extraction directory.	cpio	Updated	8.0.0.30	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3232
69	CVE-2017-7319			A vulnerability in the Linux kernel package 3.16.0-28 on Ubuntu 14.04 LTS allows any user to send a SIGIO signal to any process. If the process does not catch or ignore the signal, it will exit.	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3881
70	CVE-2017-7286			The Linux kernel package 3.16.0-28 on Ubuntu 14.04 LTS mishandles a series of mmap system calls for /dev/zero with different starting addresses, with a stated impact of allowing for a local user to possibly gain root access, aka an inode integer overflow.	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3959
71	CVE-2017-5123			A flaw was found in the upstream version of the kernels implementation of waitid systemcall. This flaw was the removal of validation of the target location where the kernel would copy the results. Previously it would implement a check to restrict the results to be copied to a valid userspace address, a new patch had inadvertently allowed copying to kernel addresses. An attacker could use this flaw to corrupt memory, panic the machine or possibly allow for arbitary memory writes.	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4205
72	CVE-2017-15107	MEDIUM	High	A vulnerability was found in the implementation of DNSSEC in Dnsmasq up to and including 2.78. Wildcard synthesized NSEC records could be improperly interpreted to prove the non-existence of hostnames that actually exist.	dnsmasq	Updated	8.0.0.25	9.0.0.25	10.17.41.20	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3216
73	CVE-2017-11146			In PHP through 5.6.31, 7.x through 7.0.21, and 7.1.x through 7.1.7, lack of bounds checks in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-11145.	php	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4646
74	CVE-2016-5875			An exploitable heap based buffer overflow exists in the handling of compressed TIFF images in LibTIFF's PixarLogDecode api. A crafted TIFF document can lead to a heap based buffer overflow resulting in remote code execution. The vulnerability can be triggered through any user controlled TIFF that is handled by this functionality.	libtiff	Updated	8.0.0.15	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3450
75	CVE-2016-5617			Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Error Handling.	mysql	Updated	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2179
76	CVE-2016-5616			Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: MyISAM.	mysql	Updated	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2169
77	CVE-2016-5320			A vulnerability was found in libtiff. A maliciously crafted TIFF file could cause the application to crash or even enable RCE on vulnerable machine when using rgb2ycbcr command.?	libtiff	Updated	8.0.0.15	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3451
78	CVE-2016-4619			libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4614, CVE-2016-4615, and CVE-2016-4616.	libxml2	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1267
79	CVE-2016-4612			libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4607, CVE-2016-4608, CVE-2016-4609, and CVE-2016-4610.	libxslt	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1262
80	CVE-2016-1515			A use-after-free / double-free vulnerability can occur in libebml master branch while parsing Track elements of the MKV container.	libebml	Updated	8.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2995
81	CVE-2016-1514			A specially crafted unicode string in libebml master branch can cause an off-by-few read on the heap in unicode string parsing code in libebml. This issue can potentially be used for information leaks.	libebml	Updated	8.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2990

	A	B	C	D	E	F	G	H	I	J	K	L	M
82	CVE-2016-0616	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-171
83	CVE-2016-0611	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-182
84	CVE-2016-0610	LOW		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-188
85	CVE-2016-0609	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to privileges.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-185
86	CVE-2016-0608	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via vectors related to UDF.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-183
87	CVE-2016-0607	LOW		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to replication.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-184
88	CVE-2016-0606	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect integrity via unknown vectors related to encryption.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-180
89	CVE-2016-0605	LOW		Unspecified vulnerability in Oracle MySQL 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-176
90	CVE-2016-0601	LOW		Unspecified vulnerability in Oracle MySQL 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Partition.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-201
91	CVE-2016-0600	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-163
92	CVE-2016-0599	LOW		Unspecified vulnerability in Oracle MySQL 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-155
93	CVE-2016-0598	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-178
94	CVE-2016-0597	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-170
95	CVE-2016-0596	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier and 5.6.27 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-191
96	CVE-2016-0595	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-157
97	CVE-2016-0594	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.21 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-203
98	CVE-2016-0546	HIGH		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Client.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-162
99	CVE-2016-0505	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Options.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-164
100	CVE-2016-0504	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0503.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-172
101	CVE-2016-0503	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0504.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-206
102	CVE-2016-0502	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-158
103													
104	**Table B:All Analyzed CVEs Affecting or Potentially Affecting WRLinux**												
105													
106	**CVE Number**	**Priority**	**CVSSv3_Severity**	**CVE Description**	**WR Comments**	**Modifications**	**Status WRLinux 8.0.0**	**Status WRLinux 9.0.0**	**Status WRLinux LTS 17**	**Status WRLinux LTS 18**	**Status WRLinux LTS 19**	**Status WRLinux CD release**	**Defect**
107	CVE-2020-9431	MEDIUM	HIGH	In Wireshark 3.2.0 to 3.2.1, 3.0.0 to 3.0.8, and 2.6.0 to 2.6.14, the LTE RRC dissector could leak memory. This was addressed in epan/dissectors/packet-lte-rrc.c by adjusting certain append operations.	wireshark	Unchanged	Not vulnerable	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4089
108	CVE-2020-9430	MEDIUM	HIGH	In Wireshark 3.2.0 to 3.2.1, 3.0.0 to 3.0.8, and 2.6.0 to 2.6.14, the WiMax DLMAP dissector could crash. This was addressed in plugins/epan/wimax/msg_dlmap.c by validating a length field.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4090
109	CVE-2020-9429	MEDIUM	HIGH	In Wireshark 3.2.0 to 3.2.1, the WireGuard dissector could crash. This was addressed in epan/dissectors/packet-wireguard.c by handling the situation where a certain data structure intentionally has a NULL value.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4091
110	CVE-2020-9428	MEDIUM	HIGH	In Wireshark 3.2.0 to 3.2.1, 3.0.0 to 3.0.8, and 2.6.0 to 2.6.14, the EAP dissector could crash. This was addressed in epan/dissectors/packet-eap.c by using more careful sscanf parsing.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4092
111	CVE-2020-9391	LOW	MEDIUM	An issue was discovered in the Linux kernel 5.4 and 5.5 through 5.5.6 on the AArch64 architecture. It ignores the top byte in the address passed to the brk system call, potentially moving the memory break downwards when the application expects it to move upwards, aka CID-dcde237319e6. This has been observed to cause heap corruption with the GNU C Library malloc implementation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-4078

	A	B	C	D	E	F	G	H	I	J	K	L	M
112	CVE-2020-9383	LOW	HIGH	An issue was discovered in the Linux kernel through 5.5.6. set_fdc in drivers/block/floppy.c leads to a wait_til_ready out-of-bounds read because the FDC index is not checked for errors before assigning it, aka CID-2e90ca68b0d2.	linux	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.7	Not vulnerable	LIN1019-4079
113	CVE-2020-9366	HIGH	CRITICAL	A buffer overflow was found in the way GNU Screen before 4.8.0 treated the special escape OSC 49. Specially crafted output, or a special program, could corrupt memory and crash Screen or possibly have unspecified other impact.	screen	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.5	Not vulnerable	LIN1019-4073
114	CVE-2020-9365	MEDIUM	HIGH	An issue was discovered in Pure-FTPd 1.0.49. An out-of-bounds (OOB) read has been detected in the pure_strcmp function in utils.c.	pure-ftpd	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4075
115	CVE-2020-9327	MEDIUM	HIGH	In SQLite 3.31.1, isAuxiliaryVtabOperator allows attackers to trigger a NULL pointer dereference and segmentation fault because of generated column optimizations.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.15	10.19.45.6	None	LIN1019-4072
116	CVE-2020-9308	MEDIUM	HIGH	archive_read_support_format_rar5.c in libarchive before 3.4.2 attempts to unpack a RAR5 file with an invalid or corrupted header (such as a header size of zero), leading to a SIGSEGV or possibly unspecified other impact.	libarchive	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.6	Not vulnerable	LIN1019-4070
117	CVE-2020-9274	MEDIUM	HIGH	An issue was discovered in Pure-FTPd 1.0.49. An uninitialized pointer vulnerability has been detected in the diraliases linked list. When the *lookup_alias(const char alias) or print_aliases(void) function is called, they fail to correctly detect the end of the linked list and try to access a non-existent list member. This is related to init_aliases in diraliases.c.	pure-ftpd	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4084
118	CVE-2020-9273	HIGH	HIGH	In ProFTPD 1.3.7, it is possible to corrupt the memory pool by interrupting the data transfer channel. This triggers a use-after-free in alloc_pool in pool.c, and possible remote code execution.	proftpd	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4068
119	CVE-2020-9272	MEDIUM	HIGH	ProFTPD 1.3.7 has an out-of-bounds (OOB) read vulnerability in mod_cap via the cap_text.c cap_to_text function.	proftpd	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4069
120	CVE-2020-8992	MEDIUM	MEDIUM	ext4_protect_reserved_inode in fs/ext4/block_validity.c in the Linux kernel through 5.5.3 allows attackers to cause a denial of service (soft lockup) via a crafted journal size.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Vulnerable	Investigate	LIN1019-4061
121	CVE-2020-8991	MEDIUM	HIGH	vg_lookup in daemons/lvmetad/lvmetad-core.c in LVM2 2.02 mismanages memory, leading to an lvmetad memory leak, as demonstrated by running pvs.	lvm2	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN1019-4062
122	CVE-2020-8835	HIGH	HIGH	In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780)	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Vulnerable	Not vulnerable	LIN1019-4231
123	CVE-2020-8834			KVM in the Linux kernel on Power8 processors has a conflicting use of HSTATE_HOST_R1 to store r1 state in kvmppc_hv_entry plus in kvmppc_{save,restore}_tm, leading to a stack corruption. Because of this, an attacker with the ability run code in kernel space of a guest VM can cause the host kernel to panic. There were two commits that, according to the reporter, introduced the vulnerability: f024ee098476 (KVM: PPC: Book3S HV: Pull out TM state save/restore into separate procedures) 87a11bb6a7f7 (KVM: PPC: Book3S HV: Work around XER[SO] bug in fake suspend mode) The former landed in 4.8, the latter in 4.17. This was fixed without realizing the impact in 4.18 with the following three commits, though it's believed the first is the only strictly necessary commit: 6f597c6b63b6 (KVM: PPC: Book3S PR: Add guest MSR parameter for kvmppc_save_tm()/kvmppc_restore_tm()) 7b0e827c6970 (KVM: PPC: Book3S HV: Factor fake-suspend handling out of kvmppc_save/restore_tm) 009c872a8bc4 (KVM: PPC: Book3S PR: Move kvmppc_save_tm/kvmppc_restore_tm to separate file)	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4268
124	CVE-2020-8832			The fix for the Linux kernel in Ubuntu 18.04 LTS for CVE-2019-14615 (The Linux kernel did not properly clear data structures on context switches for certain Intel graphics processors.) was discovered to be incomplete, meaning that in versions of the kernel before 4.15.0-91.92, an attacker could use this vulnerability to expose sensitive information.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4270
125	CVE-2020-8649	LOW	HIGH	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vgacon_invert_region function in drivers/video/console/vgacon.c.	linux	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.16	10.19.45.7	Investigate	LIN1019-4010
126	CVE-2020-8648	LOW	HIGH	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.	linux	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.7	Investigate	LIN1019-4011
127	CVE-2020-8647	LOW	HIGH	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vc_do_resize function in drivers/tty/vt/vt.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	Investigate	LIN1019-4012
128	CVE-2020-8632	LOW	MEDIUM	In cloud-init through 19.4, rand_user_password in cloudinit/config/cc_set_passwords.py has a small default pwlen value, which makes it easier for attackers to guess passwords.	cloud-init	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4044
129	CVE-2020-8631	LOW	MEDIUM	cloud-init through 19.4 relies on Mersenne Twister for a random password, which makes it easier for attackers to predict passwords, because rand_str in cloudinit/util.py calls the random.choice function.	cloud-init	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4046
130	CVE-2020-8608	HIGH	CRITICAL	In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses snprintf return values, leading to a buffer overflow in later code.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	LIN1019-4043
131	CVE-2020-8597	HIGH	CRITICAL	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions.	ppp	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.4	10.20.9.0	LIN1019-4002

	A	B	C	D	E	F	G	H	I	J	K	L	M
132	CVE-2020-8552	MEDIUM	HIGH	The Kubernetes API server component in versions prior to 1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via successful API requests.	kubernetes	Updated	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Investigate	Investigate	LIN1019-4189
133	CVE-2020-8551	LOW	MEDIUM	The Kubelet component in versions 1.15.0-1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via the kubelet API, including the unauthenticated HTTP read-only API typically served on port 10255, and the authenticated HTTPS API typically served on port 10250.	kubernetes	Updated	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Investigate	Investigate	LIN1019-4190
134	CVE-2020-8517	MEDIUM	HIGH	An issue was discovered in Squid before 4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	squid	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4008
135	CVE-2020-8492	MEDIUM	HIGH	Python 2.7 through 2.7.17, 3.5 through 3.5.9, 3.6 through 3.6.10, 3.7 through 3.7.6, and 3.8 through 3.8.1 allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking.	python	Unchanged	Vulnerable	Investigate	Investigate	Vulnerable	Investigate	Investigate	LIN1019-3979
136	CVE-2020-8450	HIGH	HIGH	An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy.	squid	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4007
137	CVE-2020-8449	MEDIUM	HIGH	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	squid	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4006
138	CVE-2020-8432	HIGH	CRITICAL	In Das U-Boot through 2020.01, a double free has been found in the cmd/gpt.c do_rename_gpt_parts() function. Double freeing may result in a write-what-where condition, allowing an attacker to execute arbitrary code. NOTE: this vulnerability was introduced when attempting to fix a memory leak identified by static analysis.	u-boot	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Vulnerable	LIN1019-4053
139	CVE-2020-8428	LOW	HIGH	fs/namei.c in the Linux kernel before 5.5 has a may_create_in_sticky use-after-free, which allows local users to cause a denial of service (OOPS) or possibly obtain sensitive information from kernel memory, aka CID-d0cb50185ae9. One attack vector may be an open system call for a UNIX domain socket, if the socket is being moved to a new parent directory and its old parent directory is being removed.	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.7	Not vulnerable	LIN1019-3978
140	CVE-2020-8112	MEDIUM	HIGH	opj_t1_clbl_decode_processor in openjp2/t1.c in OpenJPEG 2.3.1 through 2020-01-28 has a heap-based buffer overflow in the qmfbid==1 case, a different issue than CVE-2020-6851.	openjpeg	Unchanged	Won't Fix	9.0.0.25	Won't Fix	Won't Fix	10.19.45.5	None	LIN1019-3985
141	CVE-2020-8003	LOW	MEDIUM	A double-free vulnerability in vrend_renderer.c in virglrenderer through 0.8.1 allows attackers to cause a denial of service by triggering texture allocation failure, because vrend_renderer_resource_allocated_texture is not an appropriate place for a free.	virglrenderer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.4	Not vulnerable	LIN1019-3981
142	CVE-2020-8002	LOW	MEDIUM	A NULL pointer dereference in vrend_renderer.c in virglrenderer through 0.8.1 allows attackers to cause a denial of service via commands that attempt to launch a grid without previously providing a Compute Shader (CS).	virglrenderer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.4	Not vulnerable	LIN1019-3982
143	CVE-2020-7957	MEDIUM	MEDIUM	The IMAP and LMTP components in Dovecot 2.3.9 before 2.3.9.3 mishandle snippet generation when many characters must be read to compute the snippet and a trailing > character exists. This causes a denial of service in which the recipient cannot read all of their messages.	dovecot	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4037
144	CVE-2020-7919	HIGH	HIGH	Go before 1.12.16 and 1.13.x before 1.13.7 (and the crypto/cryptobyte package before 0.0.0-20200124225646-8b5121be2f68 for Go) allows attacks on clients (resulting in a panic) via a malformed X.509 certificate.	go	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4147
145	CVE-2020-7595	MEDIUM	HIGH	xmlStringLenDecodeEntities in parser.c in libxml2 2.9.10 has an infinite loop in a certain end-of-file situation.	libxml2	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.4	10.20.9.0	LIN1019-3966
146	CVE-2020-7221	HIGH	HIGH	mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently.	mariadb	Unchanged	Investigate	Investigate	Investigate	Investigate	Vulnerable	Investigate	LIN1019-4009
147	CVE-2020-7212	HIGH	HIGH	The _encode_invalid_chars function in util/url.py in the urllib3 library 1.25.2 through 1.25.7 for Python allows a denial of service (CPU consumption) because of an inefficient algorithm. The percent_encodings array contains all matches of percent encodings. It is not deduplicated. For a URL of length N, the size of percent_encodings may be up to O(N). The next step (normalize existing percent-encoded bytes) also takes up to O(N) for each step, so the total time is O(N^2). If percent_encodings were deduplicated, the time to compute _encode_invalid_chars would be O(kN), where k is at most 484 ((10+6*2)^2).	python-urllib3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.6	Won't Fix	LIN1019-4121
148	CVE-2020-7105	MEDIUM	HIGH	async.c and dict.c in libhiredis.a in hiredis through 0.14.0 allow a NULL pointer dereference because malloc return values are unchecked.	hiredis	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3933
149	CVE-2020-7066	MEDIUM	MEDIUM	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using get_headers() with user-supplied URL, if the URL contains zero (\0) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.	php	Updated	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.16	10.19.45.7	Investigate	LIN1019-4208

	A	B	C	D	E	F	G	H	I	J	K	L	M
150	CVE-2020-7065	MEDIUM	HIGH	In PHP versions 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using mb_strtolower() function with UTF-32LE encoding, certain invalid strings could cause PHP to overwrite stack-allocated buffer. This could lead to memory corruption, crashes and potentially code execution.	php	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.7	Investigate	LIN1019-4209
151	CVE-2020-7064	MEDIUM	MEDIUM	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.	php	Updated	8.0.0.33	9.0.0.25	10.17.41.21	10.18.44.16	10.19.45.7	Investigate	LIN1019-4210
152	CVE-2020-7063	MEDIUM	MEDIUM	In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when creating PHAR archive using PharData::buildFromIterator() function, the files are added with default permissions (0666, or all access) even if the original files on the filesystem were with more restrictive permissions. This may result in files having more lax permissions than intended when such archive is extracted.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.6	Investigate	LIN1019-4093
153	CVE-2020-7062	MEDIUM	HIGH	In PHP versions 7.2.x below 7.2.28, 7.3.x below 7.3.15 and 7.4.x below 7.4.3, when using file upload functionality, if upload progress tracking is enabled, but session.upload_progress.cleanup is set to 0 (disabled), and the file upload fails, the upload procedure would try to clean up data that does not exist and encounter null pointer dereference, which would likely lead to a crash.	php	Unchanged	Vulnerable	Vulnerable	10.17.41.20	10.18.44.15	10.19.45.6	Investigate	LIN1019-4094
154	CVE-2020-7061	MEDIUM	CRITICAL	In PHP versions 7.3.x below 7.3.15 and 7.4.x below 7.4.3, while extracting PHAR files on Windows using phar extension, certain content inside PHAR file could lead to one-byte read past the allocated buffer. This could potentially lead to information disclosure or crash.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.6	Investigate	LIN1019-4095
155	CVE-2020-7060	MEDIUM	CRITICAL	When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbfl_filt_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Investigate	LIN1019-4026
156	CVE-2020-7059	MEDIUM	CRITICAL	When using fgetss() function to read data with stripping tags, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause this function to read past the allocated buffer. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.5	10.20.12.0	LIN1019-4027
157	CVE-2020-7053	MEDIUM	HIGH	In the Linux kernel 4.14 longterm through 4.14.165 and 4.19 longterm through 4.19.96 (and 5.x before 5.2), there is a use-after-free (write) in the i915_ppgtt_close function in drivers/gpu/drm/i915/i915_gem_gtt.c, aka CID-7dc40713618c. This is related to i915_gem_context_destroy_ioctl in drivers/gpu/drm/i915/i915_gem_context.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.15	Not vulnerable	Not vulnerable	LIN1019-3921
158	CVE-2020-7046	HIGH	HIGH	lib-smtp in submission-login and lmtp in Dovecot 2.3.9 before 2.3.9.3 mishandles truncated UTF-8 data in command parameters, as demonstrated by the unauthenticated triggering of a submission-login infinite loop.	dovecot	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4038
159	CVE-2020-7045	MEDIUM	HIGH	In Wireshark 3.0.x before 3.0.8, the BT ATT dissector could crash. This was addressed in epan/dissectors/packet-btatt.c by validating opcodes.	wireshark	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3929
160	CVE-2020-7044	MEDIUM	HIGH	In Wireshark 3.2.x before 3.2.1, the WASSP dissector could crash. This was addressed in epan/dissectors/packet-wassp.c by using >= and <= to resolve off-by-one errors.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3930
161	CVE-2020-7039	HIGH	CRITICAL	tcp_emu in tcp_subr.c in libslirp 4.1.0, as used in QEMU 4.2.0, mismanages memory, as demonstrated by IRC DCC commands in EMU_IRC. This can cause a heap-based buffer overflow or other out-of-bounds access which can lead to a DoS or potential execute arbitrary code.	qemu	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.6	10.20.12.0	LIN1019-3957
162	CVE-2020-6851	MEDIUM	HIGH	OpenJPEG through 2.3.1 has a heap-based buffer overflow in opj_t1_clbl_decode_processor in libopenjp2.so.	openjpeg	Unchanged	Won't Fix	9.0.0.25	Won't Fix	Won't Fix	10.19.45.5	10.20.9.0	LIN1019-3922
163	CVE-2020-6750	MEDIUM	MEDIUM	GSocketClient in GNOME GLib through 2.62.4 may occasionally connect directly to a target address instead of connecting via a proxy server when configured to do so, because the proxy_addr field is mishandled. This bug is timing-dependent and may occur only sporadically depending on network delays. The greatest security relevance is in use cases where a proxy is used to help with privacy/anonymity, even though there is no technical barrier to a direct connection. NOTE: versions before 2.60 are unaffected.	glib-2.0	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.6	Investigate	LIN1019-4110
164	CVE-2020-6582	MEDIUM	HIGH	Nagios NRPE 3.2.1 has a Heap-Based Buffer Overflow, as demonstrated by interpretation of a small negative number as a large positive number during a bzero call.	nagios-nrpe	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.16	10.19.45.6	Investigate	LIN1019-4144
165	CVE-2020-6581	MEDIUM	CRITICAL	Nagios NRPE 3.2.1 has Insufficient Filtering because, for example, nasty_metachars interprets \n as the character \ and the character n (not as the \n newline sequence). This can cause command injection.	nagios-nrpe	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.16	10.19.45.6	Investigate	LIN1019-4148

	A	B	C	D	E	F	G	H	I	J	K	L	M
166	CVE-2020-6096	HIGH	CRITICAL	An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.	glibc	Updated	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4216
167	CVE-2020-5504	MEDIUM	HIGH	In phpMyAdmin 4 before 4.9.4 and 5 before 5.0.1, SQL injection exists in the user accounts page. A malicious user could inject custom SQL in place of their own username when creating queries to this page. An attacker must have a valid MySQL account to access the server.	phpmyadmin	Updated	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3909
168	CVE-2020-5496	MEDIUM	HIGH	FontForge 20190801 has a heap-based buffer overflow in the Type2NotDefSplines() function in splinesave.c.	fontforge	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3914
169	CVE-2020-5395	MEDIUM	HIGH	FontForge 20190801 has a use-after-free in SFD_GetFontMetaData in sfd.c.	fontforge	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3913
170	CVE-2020-5390	MEDIUM	HIGH	PySAML2 before 5.0.0 does not check that the signature in a SAML document is enveloped and thus signature wrapping is effective, i.e., it is affected by XML Signature Wrapping (XSW). The signature information and the node/object that is signed can be in different places and thus the signature verification will succeed, but the wrong data will be used. This specifically affects the verification of assertion that have been signed.	python-pysaml2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3923
171	CVE-2020-5313	MEDIUM	HIGH	libImaging/FliDecode.c in Pillow before 6.2.2 has an FLI buffer overflow.	python3-pillow	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	LIN1019-3906
172	CVE-2020-5312	MEDIUM	HIGH	libImaging/PcxDecode.c in Pillow before 6.2.2 has a PCX P mode buffer overflow.	python3-pillow	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	LIN1019-3905
173	CVE-2020-5311	MEDIUM	HIGH	libImaging/SgiRleDecode.c in Pillow before 6.2.2 has an SGI buffer overflow.	python3-pillow	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	LIN1019-3904
174	CVE-2020-5310	MEDIUM	HIGH	libImaging/TiffDecode.c in Pillow before 6.2.2 has a TIFF decoding integer overflow, related to realloc.	python3-pillow	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	LIN1019-3903
175	CVE-2020-5208	MEDIUM	HIGH	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	ipmitool	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.16	10.19.45.6	10.20.9.0	LIN1019-4013
176	CVE-2020-3123	MEDIUM	HIGH	A vulnerability in the Data-Loss-Prevention (DLP) module in Clam AntiVirus (ClamAV) Software versions 0.102.1 and 0.102.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to an out-of-bounds read affecting users that have enabled the optional DLP feature. An attacker could exploit this vulnerability by sending a crafted email file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.	clamav	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4045
177	CVE-2020-2694	LOW	LOW	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.18 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3937
178	CVE-2020-2686	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3938
179	CVE-2020-2679	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3939

	A	B	C	D	E	F	G	H	I	J	K	L	M
180	CVE-2020-2660	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3940
181	CVE-2020-2659	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u241 and 8u231; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11993
182	CVE-2020-2655	MEDIUM	MEDIUM	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.5 and 13.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11994
183	CVE-2020-2654	MEDIUM	LOW	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11995
184	CVE-2020-2627	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3941
185	CVE-2020-2604	MEDIUM	HIGH	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: Java). The supported version that is affected is 19.3.0.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle GraalVM Enterprise Edition. Note: GraalVM Enterprise 19.3 and above includes both Java SE 8 and Java SE 11. CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11999

	A	B	C	D	E	F	G	H	I	J	K	L	M
186	CVE-2020-2601	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-12000
187	CVE-2020-2593	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-12001
188	CVE-2020-2590	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-12002
189	CVE-2020-2589	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.28 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3944
190	CVE-2020-2588	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3945

	A	B	C	D	E	F	G	H	I	J	K	L	M
191	CVE-2020-2585	MEDIUM	MEDIUM	Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX). The supported version that is affected is Java SE: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-12013
192	CVE-2020-2584	LOW	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3946
193	CVE-2020-2583	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-12014
194	CVE-2020-2580	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3947
195	CVE-2020-2579	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.46 and prior, 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1019-3948
196	CVE-2020-2577	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3949
197	CVE-2020-2574	MEDIUM	MEDIUM	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.46 and prior, 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.6	Not vulnerable	LIN1019-3950

	A	B	C	D	E	F	G	H	I	J	K	L	M
198	CVE-2020-2573	MEDIUM	MEDIUM	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3951
199	CVE-2020-2572	MEDIUM	LOW	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plugin). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3952
200	CVE-2020-2570	MEDIUM	MEDIUM	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3953
201	CVE-2020-1934	HIGH	CRITICAL	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.	apache2	Updated	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4217
202	CVE-2020-1927	MEDIUM	MEDIUM	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.	apache2	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4218
203	CVE-2020-1747	HIGH	CRITICAL	A vulnerability was discovered in the PyYAML library in versions before 5.3.1, where it is susceptible to arbitrary code execution when it processes untrusted YAML files through the full_load method or with the FullLoader loader. Applications that use the library to process untrusted input may be vulnerable to this flaw. An attacker could use this flaw to execute arbitrary code on the system by abusing the python/object/new constructor.	python-pyyaml	Updated	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4178
204	CVE-2020-1720	LOW	MEDIUM	A flaw was found in PostgreSQL's ALTER ... DEPENDS ON EXTENSION, where sub-commands did not perform authorization checks. An authenticated attacker could use this flaw in certain configurations to perform drop objects such as function, triggers, et al., leading to database corruption. This issue affects PostgreSQL versions before 12.2, before 11.7, before 10.12 and before 9.6.17.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4152
205	CVE-2020-1712			A heap use-after-free vulnerability was found in systemd before version v245-rc1, where asynchronous Polkit queries are performed while handling dbus messages. A local unprivileged attacker can abuse this flaw to crash systemd services or potentially execute code and elevate their privileges, by sending specially crafted dbus messages.	systemd	Updated	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1019-4212
206	CVE-2020-1711	MEDIUM	CRITICAL	An out-of-bounds heap buffer access flaw was found in the way the iSCSI Block driver in QEMU versions 2.12.0 before 4.2.1 handled a response coming from an iSCSI server while checking the status of a Logical Address Block (LBA) in an iscsi_co_block_status() routine. A remote user could use this flaw to crash the QEMU process, resulting in a denial of service or potential execution of arbitrary code with privileges of the QEMU process on the host.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.15	10.19.45.5	10.20.12.0	LIN1019-4032
207	CVE-2020-11668			In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4269
208	CVE-2020-11656			In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement.	sqlite3	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4261
209	CVE-2020-11655			SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the AggInfo object's initialization is mishandled.	sqlite3	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4262
210	CVE-2020-11609	MEDIUM	MEDIUM	An issue was discovered in the stv06xx subsystem in the Linux kernel before 5.6.1. drivers/media/usb/gspca/stv06xx/stv06xx.c and drivers/media/usb/gspca/stv06xx/stv06xx_pb0100.c mishandle invalid descriptors, as demonstrated by a NULL pointer dereference, aka CID-485b06aadb93.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4253
211	CVE-2020-11608	LOW	MEDIUM	An issue was discovered in the Linux kernel before 5.6.1. drivers/media/usb/gspca/ov519.c allows NULL pointer dereferences in ov511_mode_init_regs and ov518_mode_init_regs when there are zero endpoints, aka CID-998912346c0d.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4254
212	CVE-2020-11565	MEDIUM	HIGH	An issue was discovered in the Linux kernel through 5.6.2. mpol_parse_str in mm/mempolicy.c has a stack-based out-of-bounds write because an empty nodelist is mishandled during mount option parsing, aka CID-aa9f7d5172fa.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4245

	A	B	C	D	E	F	G	H	I	J	K	L	M
213	CVE-2020-11501	MEDIUM	CRITICAL	GnuTLS 3.6.x before 3.6.13 uses incorrect cryptography for DTLS. The earliest affected version is 3.6.3 (2018-07-16) because of an error in a 2017-10-06 commit. The DTLS client always uses 32 '\0' bytes instead of a random value, and thus contributes no randomness to a DTLS negotiation. This breaks the security guarantees of the DTLS protocol.	gnutls	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4237
214	CVE-2020-11494	LOW	MEDIUM	An issue was discovered in slc_bump in drivers/net/can/slcan.c in the Linux kernel through 5.6.2. It allows attackers to read uninitialized can_frame data, potentially containing sensitive information from kernel stack memory, if the configuration lacks CONFIG_INIT_STACK_ALL, aka CID-b9258a2cece4.	linux	Updated	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1019-4230
215	CVE-2020-11441	MEDIUM	MEDIUM	** DISPUTED ** phpMyAdmin 5.0.2 allows CRLF injection, as demonstrated by %0D%0Astring%0D%0A inputs to login form fields causing CRLF sequences to be reflected on an error page. NOTE: the vendor states I don't see anything specifically exploitable.	phpmyadmin	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4211
216	CVE-2020-11102	HIGH	CRITICAL	hw/net/tulip.c in QEMU 4.2.0 has a buffer overflow during the copying of tx/rx buffers because the frame size is not validated against the r/w data length.	qemu	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4249
217	CVE-2020-10942	MEDIUM	MEDIUM	In the Linux kernel before 5.5.8, get_raw_socket in drivers/vhost/net.c lacks validation of an sk_family field, which might allow attackers to trigger kernel stack corruption via crafted system calls.	linux	Updated	8.0.0.33	9.0.0.25	Investigate	10.18.44.16	Investigate	10.20.15.0	LIN1019-4176
218	CVE-2020-10941	MEDIUM	MEDIUM	Arm Mbed TLS before 2.6.15 allows attackers to obtain sensitive information (an RSA private key) by measuring cache usage during an import.	mbedtls	Updated	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4177
219	CVE-2020-10804	MEDIUM	HIGH	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability was found in retrieval of the current username (in libraries/classes/Server/Privileges.php and libraries/classes/UserPassword.php). A malicious user with access to the server could create a crafted username, and then trick the victim into performing specific actions with that user account (such as editing its privileges).	phpmyadmin	Updated	Investigate	Investigate	Investigate	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4157
220	CVE-2020-10803	LOW	MEDIUM	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability was discovered where malicious code could be used to trigger an XSS attack through retrieving and displaying results (in tbl_get_field.php and libraries/classes/Display/Results.php). The attacker must be able to insert crafted data into certain database tables, which when retrieved (for instance, through the Browse tab) can trigger the XSS attack.	phpmyadmin	Updated	Investigate	Investigate	Investigate	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4164
221	CVE-2020-10802	MEDIUM	HIGH	In phpMyAdmin 4.x before 4.9.5 and 5.x before 5.0.2, a SQL injection vulnerability has been discovered where certain parameters are not properly escaped when generating certain queries for search actions in libraries/classes/Controllers/Table/TableSearchController.php. An attacker can generate a crafted database or table name. The attack can be performed if a user attempts certain search operations on the malicious database or table.	phpmyadmin	Updated	Investigate	Investigate	Investigate	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4165
222	CVE-2020-10648	MEDIUM	HIGH	Das U-Boot through 2020.01 allows attackers to bypass verified boot restrictions and subsequently boot arbitrary images by providing a crafted FIT image to a system configured to boot the default configuration.	u-boot	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4156
223	CVE-2020-10593	MEDIUM	HIGH	Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows remote attackers to cause a Denial of Service (memory leak), aka TROVE-2020-004. This occurs in circpad_setup_machine_on_circ because a circuit-padding machine can be negotiated twice on the same circuit.	tor	Updated	Not vulnerable	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-7115
224	CVE-2020-10592	MEDIUM	HIGH	Tor before 0.3.5.10, 0.4.x before 0.4.1.9, and 0.4.2.x before 0.4.2.7 allows remote attackers to cause a Denial of Service (CPU consumption), aka TROVE-2020-002.	tor	Updated	Not vulnerable	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-7114
225	CVE-2020-10251	MEDIUM	MEDIUM	In ImageMagick 7.0.9, an out-of-bounds read vulnerability exists within the ReadHEICImageByID function in coders\heic.c. It can be triggered via an image with a width or height value that exceeds the actual size of the image.	imagemagick	Unchanged	Investigate	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4126
226	CVE-2020-10188	HIGH	CRITICAL	utility.c in telnetd in netkit telnet through 0.17 allows remote attackers to execute arbitrary code via short writes or urgent data, because of a buffer overflow involving the netclear and nextitem functions.	netkit-telnet	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4120
227	CVE-2020-10029	LOW	MEDIUM	The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d41414141414410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c.	glibc	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	10.19.45.6	None	LIN1019-4109
228	CVE-2020-10018	MEDIUM	HIGH	WebKitGTK through 2.26.4 and WPE WebKit through 2.26.4 (which are the versions right before 2.28.0) contains a memory corruption issue (use-after-free) that may lead to arbitrary code execution. This issue has been fixed in 2.28.0 with improved memory handling.	webkitgtk	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	10.19.45.6	Investigate	LIN1019-4111
229	CVE-2020-0556	MEDIUM	HIGH	Improper access control in subsystem for BlueZ before version 5.53 may allow an unauthenticated user to potentially enable escalation of privilege and denial of service via adjacent access.	bluez5	Unchanged	Investigate	9.0.0.25	10.17.41.20	10.18.44.16	10.19.45.6	None	LIN1019-4135
230	CVE-2019-9959	Medium	MEDIUM	The JPXStream::init function in Poppler 0.78.0 and earlier doesn't check for negative values of stream length, leading to an Integer Overflow, thereby making it possible to allocate a large memory chunk on the heap, with a size controlled by an attacker, as demonstrated by pdftocairo.	poppler	Unchanged	Won't Fix	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4471

	A	B	C	D	E	F	G	H	I	J	K	L	M
231	CVE-2019-9956	Medium	HIGH	In ImageMagick 7.0.8-35 Q16, there is a stack-based buffer overflow in the function PopHexPixel of coders/ps.c, which allows an attacker to cause a denial of service or code execution via a crafted image file.	imagemagick	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3774
232	CVE-2019-9948	Medium	CRITICAL	urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call.	python	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3717
233	CVE-2019-9947	Medium	MEDIUM	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the query string or PATH_INFO) followed by an HTTP header or a Redis command. This is similar to CVE-2019-9740.	python	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-3718
234	CVE-2019-9946	Medium	HIGH	Cloud Native Computing Foundation (CNCF) CNI (Container Networking Interface) 0.7.4 has a network firewall misconfiguration which affects Kubernetes. The CNI 'portmap' plugin, used to setup HostPorts for CNI, inserts rules at the front of the iptables nat chains; which take precedence over the KUBE- SERVICES chain. Because of this, the HostPort/portmap rule could match incoming traffic even if there were better fitting, more specific service definition rules like NodePorts later in the chain. The issue is fixed in CNI 0.7.5 and Kubernetes 1.11.9, 1.12.7, 1.13.5, and 1.14.0.	cni	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3854
235	CVE-2019-9937	Medium	HIGH	In SQLite 3.27.2, interleaving reads and writes in a single transaction with an fts5 virtual table will lead to a NULL Pointer Dereference in fts5ChunkIterate in sqlite3.c. This is related to ext/fts5/fts5_hash.c and ext/fts5/fts5_index.c.	sqlite	Unchanged	Vulnerable	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3713
236	CVE-2019-9936	Medium	HIGH	In SQLite 3.27.2, running fts5 prefix queries inside a transaction could trigger a heap-based buffer over-read in fts5HashEntrySort in sqlite3.c, which may lead to an information leak. This is related to ext/fts5/fts5_hash.c.	sqlite	Unchanged	Not vulnerable	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3714
237	CVE-2019-9929	High	HIGH	Northern.tech CFEngine Enterprise 3.12.1 has Insecure Permissions.	cfengine	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4273
238	CVE-2019-9928	Medium	HIGH	GStreamer before 1.16.0 has a heap-based buffer overflow in the RTSP connection parser via a crafted response from a server, potentially allowing remote code execution.	gstreamer	Unchanged	8.0.0.31	9.0.0.21	Won't Fix	10.18.44.7	Won't Fix	Won't Fix	LIN1018-4023
239	CVE-2019-9924	HIGH	HIGH	rbash in Bash before 4.4-beta2 did not prevent the shell user from modifying BASH_CMDS, thus allowing the user to execute any command with the permissions of the shell.	bash	Updated	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3770
240	CVE-2019-9923	Medium	HIGH	pax_decode_header in sparse.c in GNU Tar before 1.32 had a NULL pointer dereference when parsing certain archives that have malformed extended headers.	tar	Unchanged	8.0.0.30	9.0.0.21	Investigate	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3716
241	CVE-2019-9917	Medium	MEDIUM	ZNC before 1.7.3-rc1 allows an existing remote user to cause a Denial of Service (crash) via invalid encoding.	znc	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3806
242	CVE-2019-9903	Medium	MEDIUM	PDFDoc::markObject in PDFDoc.cc in Poppler 0.74.0 mishandles dict marking, leading to stack consumption in the function Dict::find() located at Dict.cc, which can (for example) be triggered by passing a crafted pdf file to the pdfunite binary.	poppler	Unchanged	Won't Fix	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3764
243	CVE-2019-9893	High	CRITICAL	libseccomp before 2.4.0 did not correctly generate 64-bit syscall argument comparisons using the arithmetic operators (LT, GT, LE, GE), which might able to lead to bypassing seccomp filters and potential privilege escalations.	libseccomp	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10678
244	CVE-2019-9857	Medium	MEDIUM	In the Linux kernel through 5.0.2, the function inotify_update_existing_watch() in fs/notify/inotify/inotify_user.c neglects to call fsnotify_put_mark() with IN_MASK_CREATE after fsnotify_find_mark(), which will cause a memory leak (aka refcount leak). Finally, this will cause a denial of service.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3757
245	CVE-2019-9824	Low	MEDIUM	tcp_emu in slirp/tcp_subr.c (aka slirp/src/tcp_subr.c) in QEMU 3.0.0 uses uninitialized data in an snprintf call, leading to Information disclosure.	qemu	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4248
246	CVE-2019-9741	Medium	MEDIUM	An issue was discovered in net/http in Go 1.11.5. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the second argument to http.NewRequest with \r\n followed by an HTTP header or a Redis command.	go	Unchanged	Not vulnerable	Vulnerable	Vulnerable	Vulnerable	10.19.45.1	Not vulnerable	LIN1018-3783
247	CVE-2019-9740	Medium	MEDIUM	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n followed by an HTTP header or a Redis command.	python	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-3719
248	CVE-2019-9721	Medium	MEDIUM	A denial of service in the subtitle decoder in FFmpeg 4.1 allows attackers to hog the CPU via a crafted video file in Matroska format, because handle_open_brace in libavcodec/htmlsubtitles.c has a complex format argument to sscanf.	ffmpeg	Unchanged	Not vulnerable	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3768
249	CVE-2019-9720	High	MEDIUM	A stack-based buffer overflow in the subtitle decoder in Libav 12.3 allows attackers to corrupt the stack via a crafted video file in Matroska format, because srt_to_ass in libavcodec/srtdec.c misuses snprintf.	libav	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11547
250	CVE-2019-9719	Medium	HIGH	A stack-based buffer overflow in the subtitle decoder in Libav 12.3 allows attackers to corrupt the stack via a crafted video file in Matroska format, because srt_to_ass in libavcodec/srtdec.c misuses snprintf.	libav	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11546
251	CVE-2019-9718	Medium	MEDIUM	In FFmpeg 4.1, a denial of service in the subtitle decoder allows attackers to hog the CPU via a crafted video file in Matroska format, because ff_htmlmarkup_to_ass in libavcodec/htmlsubtitles.c has a complex format argument to sscanf.	ffmpeg	Unchanged	Not vulnerable	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3769

	A	B	C	D	E	F	G	H	I	J	K	L	M
252	CVE-2019-9717	High	MEDIUM	In Libav 12.3, a denial of service in the subtitle decoder allows attackers to hog the CPU via a crafted video file in Matroska format, because srt_to_ass in libavcodec/srtdec.c has a complex format argument to sscanf.	libav	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11545
253	CVE-2019-9675	MEDIUM	HIGH	** DISPUTED ** An issue was discovered in PHP 7.x before 7.1.27 and 7.3.x before 7.3.3. phar_tar_writeheaders_int in ext/phar/tar.c has a buffer overflow via a long link value. NOTE: The vendor indicates that the link value is used only when an archive contains a symlink, which currently cannot happen: This issue allows theoretical compromise of security, but a practical attack is usually impossible.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	Not vulnerable	Not vulnerable	LIN1019-963
254	CVE-2019-9674	HIGH	MEDIUM	Lib/zipfile.py in Python through 3.7.2 allows remote attackers to cause a denial of service (resource consumption) via a ZIP bomb.	python	Unchanged	Not vulnerable	Investigate	10.17.41.20	10.18.44.15	10.19.45.5	Not vulnerable	LIN1019-4004
255	CVE-2019-9641	High	CRITICAL	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.	php	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-3711
256	CVE-2019-9640	High	CRITICAL	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in exif_process_SOFn.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3676
257	CVE-2019-9639	High	CRITICAL	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3710
258	CVE-2019-9638	High	CRITICAL	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3679
259	CVE-2019-9637	Medium	HIGH	An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3712
260	CVE-2019-9636	Medium	CRITICAL	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.	python	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-3720
261	CVE-2019-9633	Medium	MEDIUM	gio/gsocketclient.c in GNOME GLib 2.59.2 does not ensure that a parent GTask remains alive during the execution of a connection-attempting enumeration, which allows remote attackers to cause a denial of service (g_socket_client_connected_callback mishandling and application crash) via a crafted web site, as demonstrated by GNOME Web (aka Epiphany).	glib-2.0	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3793
262	CVE-2019-9631	High	CRITICAL	Poppler 0.74.0 has a heap-based buffer over-read in the CairoRescaleBox.cc downsample_row_box_filter function.	poppler	Unchanged	Won't Fix	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3765
263	CVE-2019-9624	Medium	HIGH	Webmin 1.900 allows remote attackers to execute arbitrary code by leveraging the Java file manager and Upload and Download privileges to upload a crafted .cgi file via the /updown/upload.cgi URI.	webmin	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3787
264	CVE-2019-9553	MEDIUM	MEDIUM	Bolt 3.6.4 has XSS via the slug, teaser, or title parameter to editcontent/pages, a related issue to CVE-2017-11128 and CVE-2018-19933.	bolt	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11967
265	CVE-2019-9545	Medium	HIGH	An issue was discovered in Poppler 0.74.0. A recursive function call, in JBIG2Stream::readTextRegion() located in JBIG2Stream.cc, can be triggered by sending a crafted pdf file to (for example) the pdfimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. This is related to JBIG2Bitmap::clearToZero.	poppler	Unchanged	Won't Fix	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3700
266	CVE-2019-9543	Medium	HIGH	An issue was discovered in Poppler 0.74.0. A recursive function call, in JBIG2Stream::readGenericBitmap() located in JBIG2Stream.cc, can be triggered by sending a crafted pdf file to (for example) the pdfseparate binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. This is related to JArithmeticDecoder::decodeBit.	poppler	Unchanged	Won't Fix	Vulnerable	Won't Fix	Won't Fix	Investigate	Not vulnerable	LIN1018-3766
267	CVE-2019-9503	HIGH	HIGH	The Broadcom brcmfmac WiFi driver prior to commit a4176ec356c73a46c07c181c6d04039faf a34a9f is vulnerable to a frame validation bypass. If the brcmfmac driver receives a firmware event frame from a remote source, the is_wlc_event_frame function will cause this frame to be discarded and unprocessed. If the driver receives the firmware event frame from the host, the appropriate handler is called. This frame validation can be bypassed if the bus used is USB (for instance by a wifi dongle). This can allow firmware event frames from a remote source to be processed. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	linux	Unchanged	Not vulnerable	9.0.0.25	10.17.41.20	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3943

	A	B	C	D	E	F	G	H	I	J	K	L	M
268	CVE-2019-9500	HIGH	HIGH	The Broadcom brcmfmac WiFi driver prior to commit 1b5e2423164b3670e8bc9174e4762d297990deff is vulnerable to a heap buffer overflow. If the Wake-up on Wireless LAN functionality is configured, a malicious event frame can be constructed to trigger an heap buffer overflow in the brcmf_wowl_nd_results function. This vulnerability can be exploited with compromised chipsets to compromise the host, or when used in combination with CVE-2019-9503, can be used remotely. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	linux	Unchanged	Not vulnerable	9.0.0.25	10.17.41.20	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3942
269	CVE-2019-9499	Medium	HIGH	The implementations of EAP-PWD in wpa_supplicant EAP Peer, when built against a crypto library missing explicit validation on imported elements, do not validate the scalar and element values in EAP-pwd-Commit. An attacker may complete authentication, session key and control of the data connection with a client. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.4 are affected. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support prior to and including version 2.7 are affected.	hostapd&wpa-supplicant	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3917
270	CVE-2019-9498	Medium	HIGH	The implementations of EAP-PWD in hostapd EAP Server, when built against a crypto library missing explicit validation on imported elements, do not validate the scalar and element values in EAP-pwd-Commit. An attacker may be able to use invalid scalar/element values to complete authentication, gaining session key and network access without needing or learning the password. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.4 are affected. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support prior to and including version 2.7 are affected.	hostapd&wpa-supplicant	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3918
271	CVE-2019-9497	Medium	HIGH	The implementations of EAP-PWD in hostapd EAP Server and wpa_supplicant EAP Peer do not validate the scalar and element values in EAP-pwd-Commit. This vulnerability may allow an attacker to complete EAP-PWD authentication without knowing the password. However, unless the crypto library does not implement additional checks for the EC point, the attacker will not be able to derive the session key or complete the key exchange. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.4 are affected. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support prior to and including version 2.7 are affected.	hostapd&wpa-supplicant	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3922
272	CVE-2019-9496	Medium	HIGH	An invalid authentication sequence could result in the hostapd process terminating due to missing state validation steps when processing the SAE confirm message when in hostapd/AP mode. All version of hostapd with SAE support are vulnerable. An attacker may force the hostapd process to terminate, performing a denial of service attack. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.7 are affected.	hostapd&wpa-supplicant	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3921
273	CVE-2019-9495	Medium	LOW	The implementations of EAP-PWD in hostapd and wpa_supplicant are vulnerable to side-channel attacks as a result of cache access patterns. All versions of hostapd and wpa_supplicant with EAP-PWD support are vulnerable. The ability to install and execute applications is necessary for a successful attack. Memory access patterns are visible in a shared cache. Weak passwords may be cracked. Versions of hostapd/wpa_supplicant 2.7 and newer, are not vulnerable to the timing attack described in CVE-2019-9494. Both hostapd with EAP-pwd support and wpa_supplicant with EAP-pwd support prior to and including version 2.7 are affected.	hostapd&wpa-supplicant	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3920
274	CVE-2019-9494	Medium	MEDIUM	The implementations of SAE in hostapd and wpa_supplicant are vulnerable to side channel attacks as a result of observable timing differences and cache access patterns. An attacker may be able to gain leaked information from a side channel attack that can be used for full password recovery. Both hostapd with SAE support and wpa_supplicant with SAE support prior to and including version 2.7 are affected.	hostapd&wpa-supplicant	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3919
275	CVE-2019-9215	High	CRITICAL	In Live555 before 2019.02.27, malformed headers lead to invalid memory access in the parseAuthorizationHeader function.	live555	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3786
276	CVE-2019-9214	Medium	HIGH	In Wireshark 2.4.0 to 2.4.12 and 2.6.0 to 2.6.6, the RPCAP dissector could crash. This was addressed in epan/dissectors/packet-rpcap.c by avoiding an attempted dereference of a NULL conversation.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3721
277	CVE-2019-9213	Medium	MEDIUM	In the Linux kernel before 4.20.14, expand_downwards in mm/mmap.c lacks a check for the mmap minimum address, which makes it easier for attackers to exploit kernel NULL pointer dereferences on non-SMAP platforms. This is related to a capability check for the wrong task.	linux	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3758
278	CVE-2019-9209	Medium	HIGH	In Wireshark 2.4.0 to 2.4.12 and 2.6.0 to 2.6.6, the ASN.1 BER and related dissectors could crash. This was addressed in epan/dissectors/packet-ber.c by preventing a buffer overflow associated with excessive digits in time values.	wireshark	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3722
279	CVE-2019-9208	Medium	HIGH	In Wireshark 2.4.0 to 2.4.12 and 2.6.0 to 2.6.6, the TCAP dissector could crash. This was addressed in epan/dissectors/asn1/tcap/tcap.cnf by avoiding NULL pointer dereferences.	wireshark	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3723

	A	B	C	D	E	F	G	H	I	J	K	L	M
280	CVE-2019-9200	Medium	HIGH	A heap-based buffer underwrite exists in ImageStream::getLine() located at Stream.cc in Poppler 0.74.0 that can (for example) be triggered by sending a crafted PDF file to the pdfimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact.	poppler	Unchanged	Won't Fix	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3767
281	CVE-2019-9192	MEDIUM	HIGH	** DISPUTED ** In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1|\1)*' in grep, a different issue than CVE-2019-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-976
282	CVE-2019-9185	Medium	HIGH	Controller/Async/FilesystemManager.php in the filemanager in Bolt before 3.6.5 allows remote attackers to execute arbitrary PHP code by renaming a previously uploaded file to have a .php extension.	bolt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10686
283	CVE-2019-9169	High	CRITICAL	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match.	glibc	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3778
284	CVE-2019-9162	Medium	HIGH	In the Linux kernel before 4.20.12, net/ipv4/netfilter/nf_nat_snmp_basic_main.c in the SNMP NAT module has insufficient ASN.1 length checks (aka an array index error), making out-of-bounds read and write operations possible, leading to an OOPS or local privilege escalation. This affects snmp_version and snmp_helper.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3759
285	CVE-2019-9077	Medium	HIGH	An issue was discovered in GNU Binutils 2.32. It is a heap-based buffer overflow in process_mips_specific in readelf.c via a malformed MIPS option section.	binutils	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	10.19.45.1	Not vulnerable	LIN1018-3724
286	CVE-2019-9076	Medium	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in elf_read_notes in elf.c.	binutils	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3725
287	CVE-2019-9075	Medium	HIGH	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is a heap-based buffer overflow in _bfd_archive_64_bit_slurp_armap in archive64.c.	binutils	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	10.19.45.1	Not vulnerable	LIN1018-3726
288	CVE-2019-9074	Medium	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an out-of-bounds read leading to a SEGV in bfd_getl32 in libbfd.c, when called from pex64_get_runtime_function in pei-x86_64.c.	binutils	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	10.19.45.1	Not vulnerable	LIN1018-3727
289	CVE-2019-9073	Medium	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in _bfd_elf_slurp_version_tables in elf.c.	binutils	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	10.19.45.1	Not vulnerable	LIN1018-3728
290	CVE-2019-9072	Medium	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in setup_group in elf.c.	binutils	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3729
291	CVE-2019-9071	Medium	MEDIUM	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. It is a stack consumption issue in d_count_templates_scopes in cp-demangle.c after many recursive calls.	binutils	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	10.19.45.1	Not vulnerable	LIN1018-3730
292	CVE-2019-9070	Medium	HIGH	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. It is a heap-based buffer over-read in d_expression_1 in cp-demangle.c after many recursive calls.	binutils	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3731
293	CVE-2019-9025	High	CRITICAL	An issue was discovered in PHP 7.3.x before 7.3.1. An invalid multibyte string supplied as an argument to the mb_split() function in ext/mbstring/php_mbregex.c can cause PHP to execute memcpy() with a negative argument, which could read and write past buffers allocated for the data.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3690
294	CVE-2019-9024	Medium	HIGH	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3732
295	CVE-2019-9023	High	CRITICAL	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3707
296	CVE-2019-9022	Medium	HIGH	An issue was discovered in PHP 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.2. dns_get_record misparses a DNS response, which can allow a hostile DNS server to cause PHP to misuse memcpy, leading to read operations going past the buffer allocated for DNS data. This affects php_parserr in ext/standard/dns.c for DNS_CAA and DNS_ANY queries.	php	Unchanged	Not vulnerable	Not vulnerable	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3705
297	CVE-2019-9021	High	CRITICAL	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3691

	A	B	C	D	E	F	G	H	I	J	K	L	M
298	CVE-2019-9020	High	CRITICAL	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3692
299	CVE-2019-9003	High	HIGH	In the Linux kernel before 4.20.5, attackers can trigger a drivers/char/ipmi/ipmi_msghandler.c use-after-free and OOPS by arranging for certain simultaneous execution of the code, as demonstrated by a service ipmievd restart loop.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3760
300	CVE-2019-8980	High	HIGH	A memory leak in the kernel_read_file function in fs/exec.c in the Linux kernel through 4.20.11 allows attackers to cause a denial of service (memory consumption) by triggering vfs_read failures.	linux	Unchanged	Not vulnerable	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3761
301	CVE-2019-8956	High	HIGH	In the Linux Kernel before versions 4.20.8 and 4.19.21 a use-after-free error in the sctp_sendmsg() function (net/sctp/socket.c) when handling SCTP_SENDALL flag can be exploited to corrupt memory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3851
302	CVE-2019-8955	Medium	HIGH	In Tor before 0.3.3.12, 0.3.4.x before 0.3.4.11, 0.3.5.x before 0.3.5.8, and 0.4.x before 0.4.0.2-alpha, remote denial of service against Tor clients and relays can occur via memory exhaustion in the KIST cell scheduler.	tor	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3795
303	CVE-2019-8936	Medium	HIGH	NTP through 4.2.8p12 has a NULL Pointer Dereference.	ntp	Unchanged	8.0.0.31	Investigate	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4095
304	CVE-2019-8934	Low	LOW	hw/ppc/spapr.c in QEMU through 3.1.0 allows Information Exposure because the hypervisor shares the /proc/device-tree/system-id and /proc/device-tree/model system attributes with a guest.	qemu	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3779
305	CVE-2019-8912	High	HIGH	In the Linux kernel through 4.20.11, af_alg_release() in crypto/af_alg.c neglects to set a NULL value for a certain structure member, which leads to a use-after-free in sockfs_setattr.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.16	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3762
306	CVE-2019-8907	Medium	HIGH	do_core_note in readelf.c in libmagic.a in file 5.35 allows remote attackers to cause a denial of service (stack corruption and application crash) or possibly have unspecified other impact.	file	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3733
307	CVE-2019-8906	Medium	HIGH	do_core_note in readelf.c in libmagic.a in file 5.35 has an out-of-bounds read because memcpy is misused.	file	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3734
308	CVE-2019-8905	Medium	HIGH	do_core_note in readelf.c in libmagic.a in file 5.35 has a stack-based buffer over-read, related to file_printable, a different vulnerability than CVE-2018-10360.	file	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3735
309	CVE-2019-8904	Medium	HIGH	do_bid_note in readelf.c in libmagic.a in file 5.35 has a stack-based buffer over-read, related to file_printf and file_vprintf.	file	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3736
310	CVE-2019-8457	High	CRITICAL	SQLite3 from 3.6.0 to and including 3.27.2 is vulnerable to heap out-of-bound read in the rtreenode() function when handling invalid rtree tables.	sqlite	Unchanged	Vulnerable	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4249
311	CVE-2019-8381	Medium	HIGH	An issue was discovered in Tcpreplay 4.3.1. An invalid memory access occurs in do_checksum in checksum.c. It can be triggered by sending a crafted pcap file to the tcpreplay-edit binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact.	tcpreplay	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3771
312	CVE-2019-8377	Medium	HIGH	An issue was discovered in Tcpreplay 4.3.1. A NULL pointer dereference occurred in the function get_ipv6_l4proto() located at get.c. This can be triggered by sending a crafted pcap file to the tcpreplay-edit binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact.	tcpreplay	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3772
313	CVE-2019-8376	Medium	HIGH	An issue was discovered in Tcpreplay 4.3.1. A NULL pointer dereference occurred in the function get_layer4_v6() located at get.c. This can be triggered by sending a crafted pcap file to the tcpreplay-edit binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact.	tcpreplay	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3773
314	CVE-2019-8375	High	CRITICAL	The UIProcess subsystem in WebKit, as used in WebKitGTK through 2.23.90 and WebKitGTK+ through 2.22.6 and other products, does not prevent the script dialog size from exceeding the web view size, which allows remote attackers to cause a denial of service (Buffer Overflow) or possibly have unspecified other impact, related to UIProcess/API/gtk/WebKitScriptDialogGtk.cpp, UIProcess/API/gtk/WebKitScriptDialogImpl.cpp, and UIProcess/API/gtk/WebKitWebViewGtk.cpp, as demonstrated by GNOME Web (aka Epiphany).	webkitgtk	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-3800
315	CVE-2019-8358	Medium	HIGH	In Hiawatha before 10.8.4, a remote attacker is able to do directory traversal if AllowDotFiles is enabled.	hiawatha	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3796
316	CVE-2019-8357	Medium	MEDIUM	An issue was discovered in SoX 14.4.2. lsx_make_lpf in effect_i_dsp.c allows a NULL pointer dereference.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3746
317	CVE-2019-8356	Medium	MEDIUM	An issue was discovered in SoX 14.4.2. One of the arguments to bitrv2 in fft4g.c is not guarded, such that it can lead to write access outside of the statically declared array, aka a stack-based buffer overflow.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3747
318	CVE-2019-8355	Medium	MEDIUM	An issue was discovered in SoX 14.4.2. In xmalloc.h, there is an integer overflow on the result of multiplication fed into the lsx_valloc macro that wraps malloc. When the buffer is allocated, it is smaller than expected, leading to a heap-based buffer overflow in channels_start in remix.c.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3748
319	CVE-2019-8354	Medium	MEDIUM	An issue was discovered in SoX 14.4.2. lsx_make_lpf in effect_i_dsp.c has an integer overflow on the result of multiplication fed into malloc. When the buffer is allocated, it is smaller than expected, leading to a heap-based buffer overflow.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3749
320	CVE-2019-8343	Medium	HIGH	In Netwide Assembler (NASM) 2.14.02, there is a use-after-free in paste_tokens in asm/preproc.c.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Vulnerable	LIN1018-3788
321	CVE-2019-8337	MEDIUM	MEDIUM	In msmtp 1.8.2, when tls_trust_file has its default configuration, certificate-verification results are not properly checked.	msmtp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3574

	A	B	C	D	E	F	G	H	I	J	K	L	M
322	CVE-2019-7739	Medium	MEDIUM	An issue was discovered in Joomla! before 3.9.3. The No Filtering textfilter overrides child settings in the Global Configuration. This is intended behavior. However, it might be unexpected for the user because the configuration dialog lacks an additional message to explain this.	dialog	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3591
323	CVE-2019-7733	Medium	HIGH	In Live555 0.95, there is a buffer overflow via a large integer in a Content-Length HTTP header because handleRequestBytes has an unrestricted memmove.	live555	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3586
324	CVE-2019-7732	Medium	HIGH	In Live555 0.95, a setup packet can cause a memory leak leading to DoS because, when there are multiple instances of a single field (username, realm, nonce, uri, or response), only the last instance can ever be freed.	live555	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3595
325	CVE-2019-7665	Medium	MEDIUM	In elfutils 0.175, a heap-based buffer over-read was discovered in the function elf32_xlatetom in elf32_xlatetom.c in libelf. A crafted ELF input can cause a segmentation fault leading to denial of service (program crash) because ebl_core_note does not reject malformed core file notes.	elfutils	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3512
326	CVE-2019-7664	Medium	MEDIUM	In elfutils 0.175, a negative-sized memcpy is attempted in elf_cvt_note in libelf/note_xlate.h because of an incorrect overflow check. Crafted elf input causes a segmentation fault, leading to denial of service (program crash).	elfutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3568
327	CVE-2019-7663	MEDIUM	MEDIUM	An Invalid Address dereference was discovered in TIFFWriteDirectoryTagTransferfunction in libtiff/tif_dirwrite.c in LibTIFF 4.0.10, affecting the cpSeparateBufToContigBuf function in tiffcp.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted tiff file. This is different from CVE-2018-12900.	tiff	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3501
328	CVE-2019-7659	MEDIUM	HIGH	Genivia gSOAP 2.7.x and 2.8.x before 2.8.75 allows attackers to cause a denial of service (application abort) or possibly have unspecified other impact if a server application is built with the -DWITH_COOKIES flag. This affects the C/C++ libgsoapck/libgsoapck++ and libgsoapssl/libgsoapssl++ libraries, as these are built with that flag.	gsoap	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3537
329	CVE-2019-7638	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in Map1toN in video/SDL_pixels.c.	libsdl	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3589
330	CVE-2019-7636	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in SDL_GetRGB in video/SDL_pixels.c.	libsdl	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3522
331	CVE-2019-7578	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitIMA_ADPCM in audio/SDL_wave.c.	libsdl	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3517
332	CVE-2019-7577	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a buffer over-read in SDL_LoadWAV_RW in audio/SDL_wave.c.	libsdl	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3523
333	CVE-2019-7576	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitMS_ADPCM in audio/SDL_wave.c (outside the wNumCoef loop).	libsdl	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3580
334	CVE-2019-7575	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer overflow in MS_ADPCM_decode in audio/SDL_wave.c.	libsdl	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3505
335	CVE-2019-7574	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in IMA_ADPCM_decode in audio/SDL_wave.c.	libsdl	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3543
336	CVE-2019-7573	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitMS_ADPCM in audio/SDL_wave.c (inside the wNumCoef loop).	libsdl	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3507
337	CVE-2019-7572	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a buffer over-read in IMA_ADPCM_nibble in audio/SDL_wave.c.	libsdl	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3538
338	CVE-2019-7524	High	HIGH	In Dovecot before 2.2.36.3 and 2.3.x before 2.3.5.1, a local attacker can cause a buffer overflow in the indexer-worker process, which can be used to elevate to root. This occurs because of missing checks in the fts and pop3-uidl components.	dovecot	Unchanged	Not vulnerable	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3892
339	CVE-2019-7401	High	CRITICAL	NGINX Unit before 1.7.1 might allow an attacker to cause a heap-based buffer overflow in the router process with a specially crafted request. This may result in a denial of service (router process crash) or possibly have unspecified other impact.	nginx	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3544
340	CVE-2019-7398	Medium	HIGH	In ImageMagick before 7.0.8-25, a memory leak exists in WriteDIBImage in coders/dib.c.	imagemagick	Unchanged	8.0.0.30	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3575
341	CVE-2019-7397	Medium	HIGH	In ImageMagick before 7.0.8-25, several memory leaks exist in WritePDFImage in coders/pdf.c.	imagemagick	Unchanged	8.0.0.30	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3539
342	CVE-2019-7396	Medium	HIGH	In ImageMagick before 7.0.8-25, a memory leak exists in ReadSIXELImage in coders/sixel.c.	imagemagick	Unchanged	8.0.0.30	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3587
343	CVE-2019-7395	Medium	HIGH	In ImageMagick before 7.0.8-25, a memory leak exists in WritePSDChannel in coders/psd.c.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3500
344	CVE-2019-7317	Low	MEDIUM	png_image_free in png.c in libpng 1.6.36 has a use-after-free because png_image_free_function is called under png_safe_execute.	libpng	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3558
345	CVE-2019-7314	High	CRITICAL	liblivemedia in Live555 before 2019.02.03 mishandles the termination of an RTSP stream after RTP/RTCP-over-RTSP has been set up, which could lead to a Use-After-Free error that causes the RTSP server to crash (Segmentation fault) or possibly have unspecified other impact.	live555	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-3551
346	CVE-2019-7310	Medium	HIGH	In Poppler 0.73.0, a heap-based buffer over-read (due to an integer signedness error in the XRef::getEntry function in XRef.cc) allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document, as demonstrated by pdftocairo.	poppler	Unchanged	Won't Fix	9.0.0.20	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3536
347	CVE-2019-7309	Low	MEDIUM	In the GNU C Library (aka glibc or libc6) through 2.29, the memcmp function for the x32 architecture can incorrectly return zero (indicating that the inputs are equal) because the RDX most significant bit is mishandled.	glibc	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	10.18.44.6	10.19.45.1	Not vulnerable	LIN1018-3534

	A	B	C	D	E	F	G	H	I	J	K	L	M
348	CVE-2019-7308	HIGH	CRITICAL	kernel/bpf/verifier.c in the Linux kernel before 4.20.6 performs undesirable out-of-bounds speculation on pointer arithmetic in various cases, including cases of different branches with different state or limits to sanitize, leading to side-channel attacks.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3545
349	CVE-2019-7283	MEDIUM	MEDIUM	An issue was discovered in rcp in NetKit through 0.17. For an rcp operation, the server chooses which files/directories are sent to the client. However, the rcp client only performs cursory validation of the object name returned. A malicious rsh server (or Man-in-The-Middle attacker) can overwrite arbitrary files in a directory on the rcp client machine. This is similar to CVE-2019-6111.	netkit-rsh	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	10.19.45.1	Not vulnerable	LIN1018-3541
350	CVE-2019-7282	MEDIUM	MEDIUM	In NetKit through 0.17, rcp.c in the rcp client allows remote rsh servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side. This is similar to CVE-2018-20685.	netkit-rsh	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	10.19.45.1	Not vulnerable	LIN1018-3510
351	CVE-2019-7222	LOW	MEDIUM	An information leakage issue was found in the way Linux kernel's KVM hypervisor handled page fault exception while emulating instructions like VMXON, VMCLEAR, VMPTRLD, VMWRITE with memory address as an operand. It occurs if the operand is an mmio address, as the returned exception object holds uninitialised stack memory Contents.	linux	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3553
352	CVE-2019-7221	MEDIUM	HIGH	A use after free issue was found in the way Linux kernel's KVM hypervisor emulates a preemption timer for L2 guest when nested(=1) virtualization is enabled. This high resolution timer(hrtimer) runs when L2 guest is active. After VM exit, in sync_vmcs12() timer object is stopped. The use-after-free occurs if the timer object is free'd before calling sync_vmcs12() routine.	linux	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3576
353	CVE-2019-7175	Medium	HIGH	In ImageMagick before 7.0.8-25, some memory leaks exist in DecodeImage in coders/pcd.c.	imagemagick	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3775
354	CVE-2019-7150	Medium	MEDIUM	An issue was discovered in elfutils 0.175. A segmentation fault can occur in the function elf64_xlatetom in libelf/elf32_xlatetom.c, due to dwfl_segment_report_module not checking whether the dyn data read from a core file is truncated. A crafted input can cause a program crash, leading to denial-of-service, as demonstrated by eu-stack.	elfutils	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3548
355	CVE-2019-7149	Medium	MEDIUM	A heap-based buffer over-read was discovered in the function read_srclines in dwarf_getsrclines.c in libdw in elfutils 0.175. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by eu-nm.	elfutils	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3563
356	CVE-2019-7148	Medium	MEDIUM	An attempted excessive memory allocation was discovered in the function read_long_names in elf_begin.c in libelf in elfutils 0.174. Remote attackers could leverage this vulnerability to cause a denial-of-service via crafted elf input, which leads to an out-of-memory exception.	elfutils	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3496
357	CVE-2019-7147	Medium	MEDIUM	A buffer over-read exists in the function crc64ib in crc64.c in nasmlib in Netwide Assembler (NASM) 2.14rc16. A crafted asm input can cause segmentation faults, leading to denial-of-service.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-3509
358	CVE-2019-7146	Medium	MEDIUM	In elfutils 0.175, there is a buffer over-read in the ebl_object_note function in eblobjnote.c in libebl. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted elf file, as demonstrated by eu-readelf.	elfutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3520
359	CVE-2019-6988	Medium	MEDIUM	An issue was discovered in OpenJPEG 2.3.0. It allows remote attackers to cause a denial of service (attempted excessive memory allocation) in opj_calloc in openjp2/opj_malloc.c, when called from opj_tcd_init_tile in openjp2/tcd.c, as demonstrated by the 64-bit opj_decompress.	openjpeg	Unchanged	Won't Fix	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3592
360	CVE-2019-6978	High	CRITICAL	The GD Graphics Library (aka LibGD) 2.2.5 has a double free in the gdImage*Ptr() functions in gd_gif_out.c, gd_jpeg.c, and gd_wbmp.c. NOTE: PHP is unaffected.	gd	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	10.19.45.1	Not vulnerable	LIN1018-3570
361	CVE-2019-6977	Medium	HIGH	gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger imagecolormatch calls with crafted image data.	php	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3562
362	CVE-2019-6974	MEDIUM	HIGH	A use after free issue was found in the way Linux kernel's KVM hypervisor implements its device control API. While creating a device via kvm_ioctl_create_device(), device holds a reference to a VM object, latter this reference is transferred to caller's file descriptor table. If such file descriptor was to be closed, reference count to the VM object could become zero, potentially leading to use-after-free issue latter.	linux	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3585
363	CVE-2019-6956	Medium	HIGH	An issue was discovered in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. It is a buffer over-read in ps_mix_phase in libfaad/ps_dec.c.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3546
364	CVE-2019-6799	Medium	MEDIUM	An issue was discovered in phpMyAdmin before 4.8.5. When the AllowArbitraryServer configuration setting is set to true, with the use of a rogue MySQL server, an attacker can read any file on the server that the web server's user can access. This is related to the mysql.allow_local_infile PHP configuration, and the inadvertent ignoring of options(MYSQLI_OPT_LOCAL_INFILE calls.	phpmyadmin	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3518
365	CVE-2019-6798	High	CRITICAL	An issue was discovered in phpMyAdmin before 4.8.5. A vulnerability was reported where a specially crafted username can be used to trigger a SQL injection attack through the designer feature.	phpmyadmin	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3594

	A	B	C	D	E	F	G	H	I	J	K	L	M
366	CVE-2019-6778	MEDIUM	HIGH	A heap buffer overflow issue was found in the SLiRP networking implementation of the QEMU emulator. It occurs in tcp_emu() routine while emulating Identification protocol and copying message data to a socket buffer.	qemu	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3555
367	CVE-2019-6706	Medium	HIGH	Lua 5.3.5 has a use-after-free in lua_upvaluejoin in lapi.c. For example, a crash outcome might be achieved by an attacker who is able to trigger a debug.upvaluejoin call in which the arguments have certain relationships.	lua	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3527
368	CVE-2019-6502	High	CRITICAL	sc_context_create in ctx.c in libopensc in OpenSC 0.19.0 has a memory leak, as demonstrated by a call from eidenv.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3524
369	CVE-2019-6501	LOW	MEDIUM	An out of bounds r/w access issue was found in the way QEMU handled inquiry request coming from a guest in scsi_handle_inquiry_reply(). A guest user/process could use this flaw to corrupt byte of QEMU process Memory.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3526
370	CVE-2019-6488	Medium	HIGH	The string component in the GNU C Library (aka glibc or libc6) through 2.28, when running on the x32 architecture, incorrectly attempts to use a 64-bit register for size_t in assembly codes, which can lead to a segmentation fault or possibly unspecified other impact, as demonstrated by a crash in __memmove_avx_unaligned_erms in sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S during a memcpy.	glibc	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3495
371	CVE-2019-6486	High	HIGH	Go before 1.10.8 and 1.11.x before 1.11.5 mishandles P-521 and P-384 elliptic curves, which allows attackers to cause a denial of service (CPU consumption) or possibly conduct ECDH private key recovery attacks.	go	Unchanged	Not vulnerable	Not vulnerable	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3598
372	CVE-2019-6476	MEDIUM	HIGH	A defect in code added to support QNAME minimization can cause named to exit with an assertion failure if a forwarder returns a referral rather than resolving the query. This affects BIND versions 9.14.0 up to 9.14.6, and 9.15.0 up to 9.15.4.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1018-5143
373	CVE-2019-6475	MEDIUM	HIGH	Mirror zones are a BIND feature allowing recursive servers to pre-cache zone data provided by other servers. A mirror zone is similar to a zone of type secondary, except that its data is subject to DNSSEC validation before being used in answers, as if it had been looked up via traditional recursion, and when mirror zone data cannot be validated, BIND falls back to using traditional recursion instead of the mirror zone. However, an error in the validity checks for the incoming zone data can allow an on-path attacker to replace zone data that was validated with a configured trust anchor with forged data of the attacker's choosing. The mirror zone feature is most often used to serve a local copy of the root zone. If an attacker was able to insert themselves into the network path between a recursive server using a mirror zone and a root name server, this vulnerability could then be used to cause the recursive server to accept a copy of falsified root zone data. This affects BIND versions 9.14.0 up to 9.14.6, and 9.15.0 up to 9.15.4.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1018-5144
374	CVE-2019-6471	MEDIUM	MEDIUM	A race condition which may occur when discarding malformed packets can result in BIND exiting due to a REQUIRE assertion failure in dispatch.c. Versions affected: BIND 9.11.0 -> 9.11.7, 9.12.0 -> 9.12.4-P1, 9.14.0 -> 9.14.2. Also all releases of the BIND 9.13 development branch and version 9.15.0 of the BIND 9.15 development branch and BIND Supported Preview Edition versions 9.11.3-S1 -> 9.11.7-S1.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.12	10.19.45.1	Not vulnerable	LIN1018-5071
375	CVE-2019-6470	MEDIUM	HIGH	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source, or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1019-3299
376	CVE-2019-6469	MEDIUM	HIGH	An error in the EDNS Client Subnet (ECS) feature for recursive resolvers can cause BIND to exit with an assertion failure when processing a response that has malformed RRSIGs. Versions affected: BIND 9.10.5-S1 -> 9.11.6-S1 of BIND 9 Supported Preview Edition.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5082
377	CVE-2019-6468	MEDIUM	HIGH	In BIND Supported Preview Edition, an error in the nxdomain-redirect feature can occur in versions which support EDNS Client Subnet (ECS) features. In those versions which have ECS support, enabling nxdomain-redirect is likely to lead to BIND exiting due to assertion failure. Versions affected: BIND Supported Preview Edition version 9.10.5-S1 -> 9.11.5-S5. ONLY BIND Supported Preview Edition releases are affected.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5075

	A	B	C	D	E	F	G	H	I	J	K	L	M
378	CVE-2019-6465	MEDIUM	MEDIUM	Controls for zone transfers may not be properly applied to Dynamically Loadable Zones (DLZs) if the zones are writable Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P2, 9.12.0 -> 9.12.3-P2, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2019-6465.	bind	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5077
379	CVE-2019-6462	Medium	MEDIUM	An issue was discovered in cairo 1.16.0. There is an infinite loop in the function _arc_error_normalized in the file cairo-arc.c, related to _arc_max_angle_for_tolerance_normalized.	cairo	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	10.19.45.1	Not vulnerable	LIN1018-3565
380	CVE-2019-6461	Medium	MEDIUM	An issue was discovered in cairo 1.16.0. There is an assertion problem in the function _cairo_arc_in_direction in the file cairo-arc.c.	cairo	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	10.19.45.1	Not vulnerable	LIN1018-3554
381	CVE-2019-6454	MEDIUM	MEDIUM	An issue was discovered in sd-bus in systemd 239. bus_process_object() in libsystemd/sd-bus/bus-objects.c allocates a variable-length stack buffer for temporarily storing the object path of incoming D-Bus messages. An unprivileged local user can exploit this by sending a specially crafted message to PID1, causing the stack pointer to jump over the stack guard pages into an unmapped memory region and trigger a denial of service (systemd PID1 crash and kernel panic).	systemd	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3782
382	CVE-2019-6439	High	CRITICAL	examples/benchmark/tls_bench.c in a benchmark tool in wolfSSL through 3.15.7 has a heap-based buffer overflow.	wolfssl	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3588
383	CVE-2019-6293	MEDIUM	MEDIUM	An issue was discovered in the function mark_beginning_as_normal in nfa.c in flex 2.6.4. There is a stack exhaustion problem caused by the mark_beginning_as_normal function making recursive calls to itself in certain scenarios involving lots of '*' characters. Remote attackers could leverage this vulnerability to cause a denial-of-service.	flex	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-3388
384	CVE-2019-6291	MEDIUM	MEDIUM	An issue was discovered in the function expr6 in eval.c in Netwide Assembler (NASM) through 2.14.02. There is a stack exhaustion problem caused by the expr6 function making recursive calls to itself in certain scenarios involving lots of '!' or '+' or '-' characters. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted asm file.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-3384
385	CVE-2019-6290	MEDIUM	MEDIUM	An infinite recursion issue was discovered in eval.c in Netwide Assembler (NASM) through 2.14.02. There is a stack exhaustion problem resulting from infinite recursion in the functions expr, rexp, bexpr and cexpr in certain scenarios involving lots of '(' characters. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted asm file.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-3401
386	CVE-2019-6256	HIGH	CRITICAL	A Denial of Service issue was discovered in the LIVE555 Streaming Media libraries as used in Live555 Media Server 0.93. It can cause an RTSPServer crash in handleHTTPCmd_TunnelingPOST, when RTSP-over-HTTP tunneling is supported, via x-sessioncookie HTTP headers in a GET request and a POST request within the same TCP session. This occurs because of a call to an incorrect virtual function pointer in the readSocket function in GroupsockHelper.cpp.	live555	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3411
387	CVE-2019-6250	HIGH	HIGH	A pointer overflow, with code execution, was discovered in ZeroMQ libzmq (aka 0MQ) 4.2.x and 4.3.x before 4.3.1. A v2_decoder.cpp zmq::v2_decoder_t::size_ready integer overflow allows an authenticated attacker to overwrite an arbitrary amount of bytes beyond the bounds of a buffer, which can be leveraged to run arbitrary code on the target system. The memory layout allows the attacker to inject OS commands into a data structure located immediately after the problematic buffer (i.e., it is not necessary to use a typical buffer-overflow exploitation technique that changes the flow of control).	zeromq	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3413
388	CVE-2019-6133	MEDIUM	MEDIUM	In PolicyKit (aka polkit) 0.115, the start time protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in polkitbackend/polkitbackendinteractiveauthority.c.	polkit	Unchanged	Not vulnerable	9.0.0.20	10.17.41.14	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3395
389	CVE-2019-6129	MEDIUM	HIGH	png_create_info_struct in png.c in libpng 1.6.36 has a memory leak, as demonstrated by pngcp.	libpng	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Won't Fix	Won't Fix	LIN1018-3378
390	CVE-2019-6128	MEDIUM	HIGH	The TIFFFdOpen function in tif_unix.c in LibTIFF 4.0.10 has a memory leak, as demonstrated by pal2rgb.	tiff	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3397
391	CVE-2019-6116	MEDIUM	HIGH	It was discovered that the ghostscript /invalidaccess checks fail under certain conditions. An attacker could possibly exploit this to bypass the -dSAFER protection and, for example, execute arbitrary shell commands via a specially crafted PostScript document.	ghostscript	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3559
392	CVE-2019-6111	MEDIUM	MEDIUM	OpenSSH has a vulnerability in the scp client utility. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, scp client only perform cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example overwrite .ssh/authorized_keys).	openssh	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3394
393	CVE-2019-6110	MEDIUM	MEDIUM	OpenSSH has a vulnerability in the scp client utility. Due to accepting and displaying arbitrary stderr output from the scp server, a malicious server can manipulate the client output, for example to employ ANSI codes to hide additional files being transferred.	openssh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3415

	A	B	C	D	E	F	G	H	I	J	K	L	M
394	CVE-2019-6109	MEDIUM	MEDIUM	OpenSSH has a vulnerability in the scp client utility. Due to missing character encoding in the progress display, the object name can be used to manipulate the client output, for example to employ ANSI codes to hide additional files being transferred.	openssh	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3392
395	CVE-2019-5953	High	CRITICAL	Buffer overflow in GNU Wget 1.20.1 and earlier allows remote attackers to cause a denial-of-service (DoS) or may execute an arbitrary code via unspecified vectors.	wget	Unchanged	8.0.0.31	Investigate	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4094
396	CVE-2019-5882	HIGH	CRITICAL	Irssi 1.1.x before 1.1.2 has a use after free when hidden lines are expired from the scroll buffer.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3377
397	CVE-2019-5815	MEDIUM	HIGH	Type confusion in xsltNumberFormatGetMultipleLevel prior to libxslt 1.1.33 could allow attackers to potentially exploit heap corruption via crafted XML data.	libxslt	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3745
398	CVE-2019-5747	MEDIUM	HIGH	An issue was discovered in BusyBox through 1.30.0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and/or relay) might allow a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to assurance of a 4-byte length when decoding DHCP_SUBNET. NOTE: this issue exists because of an incomplete fix for CVE-2018-20679.	busybox	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3374
399	CVE-2019-5736	HIGH	HIGH	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.	runc	Unchanged	Not vulnerable	9.0.0.20	10.17.41.15	10.18.44.5	10.19.45.1	Not vulnerable	LIN1018-3597
400	CVE-2019-5721	MEDIUM	MEDIUM	In Wireshark 2.4.0 to 2.4.11, the ENIP dissector could crash. This was addressed in epan/dissectors/packet-enip.c by changing the memory-management approach so that a use-after-free is avoided.	wireshark	Unchanged	Vulnerable	9.0.0.20	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3383
401	CVE-2019-5719	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the ISAKMP dissector could crash. This was addressed in epan/dissectors/packet-isakmp.c by properly handling the case of a missing decryption data block.	wireshark	Unchanged	8.0.0.30	9.0.0.20	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3382
402	CVE-2019-5718	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the RTSE dissector and other ASN.1 dissectors could crash. This was addressed in epan/charsets.c by adding a get_t61_string length check.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3381
403	CVE-2019-5717	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the P_MUL dissector could crash. This was addressed in epan/dissectors/packet-p_mul.c by rejecting the invalid sequence number of zero.	wireshark	Unchanged	8.0.0.30	9.0.0.20	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3380
404	CVE-2019-5716	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.5, the 6LoWPAN dissector could crash. This was addressed in epan/dissectors/packet-6lowpan.c by avoiding use of a TVB before its creation.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3410
405	CVE-2019-5489	LOW	MEDIUM	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3403
406	CVE-2019-5482	High	CRITICAL	Heap buffer overflow in the TFTP protocol handler in cURL 7.19.4 to 7.65.3.	curl	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-5056
407	CVE-2019-5481	High	CRITICAL	Double-free vulnerability in the FTP-kerberos code in cURL 7.52.0 to 7.65.3.	curl	Unchanged	Not vulnerable	Not vulnerable	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-5055
408	CVE-2019-5459	MEDIUM	HIGH	An Integer underflow in VLC Media Player versions < 3.0.7 leads to an out-of-band read.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4598
409	CVE-2019-5443	Medium	HIGH	A non-privileged user or program can put code and a config file in a known non-privileged path (under C:/usr/local/) that will make curl <= 7.65.1 automatically run the code (as an openssl engine) on invocation. If that curl is invoked by a privileged user it can do anything it wants.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4384
410	CVE-2019-5436	Medium	HIGH	A heap buffer overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl versions 7.19.4 through 7.64.1.	curl	Unchanged	8.0.0.31	Investigate	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4171
411	CVE-2019-5435	Medium	LOW	An integer overflow in curl's URL API results in a buffer overflow in libcurl 7.62.0 to and including 7.64.1.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4172
412	CVE-2019-5108	LOW	MEDIUM	An exploitable denial-of-service vulnerability exists in the Linux kernel prior to mainline 5.3. An attacker could exploit this vulnerability by triggering AP to send IAPP location updates for stations before the required authentication process has completed. This could lead to different denial-of-service scenarios, either by causing CAM table attacks, or by leading to traffic flapping if faking already existing clients in other nearby APs of the same wireless infrastructure. An attacker can forge Authentication and Association Request packets to trigger this vulnerability.	linux	Unchanged	Vulnerable	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN1019-3880
413	CVE-2019-5094	Medium	MEDIUM	An exploitable code execution vulnerability exists in the quota file functionality of E2fsprogs 1.45.3. A specially crafted ext4 partition can cause an out-of-bounds write on the heap, resulting in code execution. An attacker can corrupt a partition to trigger this vulnerability.	e2fsprogs	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	10.19.45.1	Not vulnerable	LIN1018-5006
414	CVE-2019-5063	MEDIUM	HIGH	An exploitable heap buffer overflow vulnerability exists in the data structure persistence functionality of OpenCV 4.1.0. A specially crafted XML file can cause a buffer overflow, resulting in multiple heap corruptions and potential code execution. An attacker can provide a specially crafted file to trigger this vulnerability.	opencv	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3885

	A	B	C	D	E	F	G	H	I	J	K	L	M
415	CVE-2019-5062	LOW	MEDIUM	An exploitable denial-of-service vulnerability exists in the 802.11w security state handling for hostapd 2.6 connected clients with valid 802.11w sessions. By simulating an incomplete new association, an attacker can trigger a deauthentication against stations using 802.11w, resulting in a denial of service.	hostapd&wpa-supplicant	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Investigate	LIN1019-3780
416	CVE-2019-5061	LOW	MEDIUM	An exploitable denial-of-service vulnerability exists in the hostapd 2.6, where an attacker could trigger AP to send IAPP location updates for stations, before the required authentication process has completed. This could lead to different denial of service scenarios, either by causing CAM table attacks, or by leading to traffic flapping if faking already existing clients in other nearby Aps of the same wireless infrastructure. An attacker can forge Authentication and Association Request packets to trigger this vulnerability.	hostapd&wpa-supplicant	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Investigate	LIN1019-3779
417	CVE-2019-5060	Medium	HIGH	An exploitable code execution vulnerability exists in the XPM image rendering function of SDL2_image 2.0.4. A specially crafted XPM image can cause an integer overflow in the colorhash function, allocating too small of a buffer. This buffer can then be written out of bounds, resulting in a heap overflow, ultimately ending in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	libsdl2-image	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4592
418	CVE-2019-5059	Medium	HIGH	An exploitable code execution vulnerability exists in the XPM image rendering functionality of SDL2_image 2.0.4. A specially crafted XPM image can cause an integer overflow, allocating too small of a buffer. This buffer can then be written out of bounds resulting in a heap overflow, ultimately ending in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	libsdl2-image	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4593
419	CVE-2019-5058	Medium	HIGH	An exploitable code execution vulnerability exists in the XCF image rendering functionality of SDL2_image 2.0.4. A specially crafted XCF image can cause a heap overflow, resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	libsdl2-image	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4594
420	CVE-2019-5057	Medium	HIGH	An exploitable code execution vulnerability exists in the PCX image-rendering functionality of SDL2_image 2.0.4. A specially crafted PCX image can cause a heap overflow, resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	libsdl2-image	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4595
421	CVE-2019-5052	Medium	HIGH	An exploitable integer overflow vulnerability exists when loading a PCX file in SDL2_image 2.0.4. A specially crafted file can cause an integer overflow, resulting in too little memory being allocated, which can lead to a buffer overflow and potential code execution. An attacker can provide a specially crafted image file to trigger this vulnerability.	libsdl2-image	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4390
422	CVE-2019-5051	Medium	HIGH	An exploitable heap-based buffer overflow vulnerability exists when loading a PCX file in SDL2_image, version 2.0.4. A missing error handler can lead to a buffer overflow and potential code execution. An attacker can provide a specially crafted image file to trigger this vulnerability.	libsdl2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4391
423	CVE-2019-5018	Medium	HIGH	An exploitable use after free vulnerability exists in the window function functionality of Sqlite3 3.26.0. A specially crafted SQL command can cause a use after free vulnerability, potentially resulting in remote code execution. An attacker can send a malicious SQL command to trigger this vulnerability.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4063
424	CVE-2019-5010	MEDIUM	HIGH	An exploitable denial-of-service vulnerability exists in the X509 certificate parser of Python.org Python 2.7.11 / 3.7.2. A specially crafted X509 certificate can cause a NULL pointer dereference, resulting in a denial of service. An attacker can initiate or accept TLS connections using crafted certificates to trigger this vulnerability.	python	Unchanged	8.0.0.30	9.0.0.20	Investigate	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3502
425	CVE-2019-5008	Medium	HIGH	hw/sparc64/sun4u.c in QEMU 3.1.50 is vulnerable to a NULL pointer dereference, which allows the attacker to cause a denial of service via a device driver.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3929
426	CVE-2019-3902	Medium	MEDIUM	A flaw was found in Mercurial before 4.9. It was possible to use symlinks and subrepositories to defeat Mercurial's path-checking logic and write files outside a repository.	mercurial	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4026
427	CVE-2019-3901	Low	MEDIUM	A race condition in perf_event_open() allows local attackers to leak sensitive data from setuid programs. As no relevant locks (in particular the cred_guard_mutex) are held during the ptrace_may_access() call, it is possible for the specified target task to perform an execve() syscall with setuid execution before perf_event_alloc() actually attaches to it, allowing an attacker to bypass the ptrace_may_access() check and the perf_event_exit_task(current) call that is performed in install_exec_creds() during privileged execve() calls. This issue affects kernel versions before 4.8.	linux	Unchanged	8.0.0.33	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4052
428	CVE-2019-3900	Medium	MEDIUM	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A guest user, maybe remote one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.	linux	Unchanged	Vulnerable	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4041
429	CVE-2019-3896	High	HIGH	A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service (DoS).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4297

	A	B	C	D	E	F	G	H	I	J	K	L	M
430	CVE-2019-3887	Medium	MEDIUM	A flaw was found in the way KVM hypervisor handled x2APIC Machine Specific Rregister (MSR) access with nested(=1) virtualization enabled. In that, L1 guest could access L0's APIC register values via L2 guest, when 'virtualize x2APIC mode' is enabled. A guest could use this flaw to potentially crash the host kernel resulting in DoS issue. Kernel versions from 4.16 and newer are vulnerable to this issue.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4180
431	CVE-2019-3886	Medium	MEDIUM	An incorrect permissions check was discovered in libvirt 4.8.0 and above. The readonly permission was allowed to invoke APIs depending on the guest agent, which could lead to potentially disclosing unintended information or denial of service by causing libvirt to block.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3849
432	CVE-2019-3885	Medium	HIGH	A use-after-free flaw was found in pacemaker up to and including version 2.0.1 which could result in certain sensitive information to be leaked via the system logs.	pacemaker	Unchanged	Vulnerable	Vulnerable	Vulnerable	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3942
433	CVE-2019-3882	Medium	MEDIUM	A flaw was found in the Linux kernel's vfio interface implementation that permits violation of the user's locked memory limit. If a device is bound to a vfio driver, such as vfio-pci, and the local attacker is administratively granted ownership of the device, it may cause a system memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4042
434	CVE-2019-3880	Medium	MEDIUM	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.	samba	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3886
435	CVE-2019-3870	Low	MEDIUM	A vulnerability was found in Samba from version (including) 4.9 to versions before 4.9.6 and 4.10.2. During the creation of a new Samba AD DC, files are created in a private subdirectory of the install location. This directory is typically mode 0700, that is owner (root) only access. However in some upgraded installations it will have other permissions, such as 0755, because this was the default before Samba 4.8. Within this directory, files are created with mode 0666, which is world-writable, including a sample krb5.conf, and the list of DNS names and servicePrincipalName values to update.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3887
436	CVE-2019-3863	Medium	HIGH	A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out of bounds memory write error.	libssh2	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3737
437	CVE-2019-3862	Medium	CRITICAL	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	libssh2	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-3738
438	CVE-2019-3861	Medium	CRITICAL	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	libssh2	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-3739
439	CVE-2019-3860	Medium	CRITICAL	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	libssh2	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-3740
440	CVE-2019-3859	Medium	CRITICAL	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	libssh2	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-3741
441	CVE-2019-3858	Medium	CRITICAL	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.	libssh2	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-3742
442	CVE-2019-3857	Medium	HIGH	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.	libssh2	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3743
443	CVE-2019-3856	Medium	HIGH	An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.	libssh2	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3744
444	CVE-2019-3855	High	HIGH	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.	libssh2	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3745
445	CVE-2019-3846	High	HIGH	A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifiex kernel module while connecting to a malicious wireless network.	linux	Unchanged	Not vulnerable	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4251

	A	B	C	D	E	F	G	H	I	J	K	L	M
446	CVE-2019-3842	Medium	HIGH	In systemd before v242-rc4, it was discovered that pam_systemd does not properly sanitize the environment before using the XDG_SEAT variable. It is possible for an attacker, in some particular configurations, to set a XDG_SEAT environment variable which allows for commands to be checked against polkit policies using the allow_active element rather than allow_any.	systemd	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3885
447	CVE-2019-3840	Low	MEDIUM	A NULL pointer dereference flaw was discovered in libvirt before version 5.0.0 in the way it gets interface information through the QEMU agent. An attacker in a guest VM can use this flaw to crash libvirtd and cause a denial of service.	libvirt	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3810
448	CVE-2019-3839	Medium	HIGH	It was found that in ghostscript some privileged operators remained accessible from various places after the CVE-2019-6116 fix. A specially crafted PostScript file could use this flaw in order to, for example, have access to the file system outside of the constrains imposed by -dSAFER. Ghostscript versions before 9.27 are vulnerable.	ghostscript	Unchanged	Investigate	9.0.0.24	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4097
449	CVE-2019-3838	MEDIUM	MEDIUM	It was found that the forceput operator could be extracted from the DefineResource method in ghostscript before 9.27. A specially crafted PostScript file could use this flaw in order to, for example, have access to the file system outside of the constrains imposed by -dSAFER.	ghostscript	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	10.19.45.1	Not vulnerable	LIN1018-3750
450	CVE-2019-3836	Medium	HIGH	It was discovered in gnutls before version 3.6.7 upstream that there is an uninitialized pointer access in gnutls versions 3.6.3 or later which can be triggered by certain post-handshake messages.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3846
451	CVE-2019-3835	MEDIUM	MEDIUM	It was found that the superexec operator was available in the internal dictionary in ghostscript before 9.27. A specially crafted PostScript file could use this flaw in order to, for example, have access to the file system outside of the constrains imposed by -dSAFER.	ghostscript	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	10.19.45.1	Not vulnerable	LIN1018-3751
452	CVE-2019-3833	Medium	HIGH	Openwsman, versions up to and including 2.6.9, are vulnerable to infinite loop in process_connection() when parsing specially crafted HTTP requests. A remote, unauthenticated attacker can exploit this vulnerability by sending malicious HTTP request to cause denial of service to openwsman server.	openwsman	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3776
453	CVE-2019-3832	LOW	MEDIUM	It was discovered the fix for CVE-2018-19758 is not complete and it still allows to read beyond the limit of the buffer in function wav_write_header() in wav.c. Function wav_write_header() iterates through the `loops` array for an amount of times read from the file itself. However, this value is not correctly checked and the library can read beyond the limits of the `loops` array, possibly making the application crash.	libsndfile	Unchanged	Investigate	9.0.0.21	10.17.41.15	10.18.44.5	10.19.45.1	Not vulnerable	LIN1018-3578
454	CVE-2019-3831	High	HIGH	A vulnerability was discovered in vdsm, version 4.19 through 4.30.3 and 4.30.5 through 4.30.8. The systemd_run function exposed to the vdsm system user could be abused to execute arbitrary commands as root.	vdsm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	New
455	CVE-2019-3829	Medium	HIGH	A vulnerability was found in gnutls versions from 3.5.8 before 3.6.7. A memory corruption (double free) vulnerability in the certificate verification API. Any client or server application that verifies X.509 certificates with GnuTLS 3.5.8 or later is affected.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Vulnerable	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3809
456	CVE-2019-3827	Low	MEDIUM	An incorrect permission check in the admin backend in gvfs before version 1.39.4 was found that allows reading and modify arbitrary files by privileged users without asking for password when no authentication agent is running. This vulnerability can be exploited by malicious programs running under privileges of users belonging to the wheel group to further escalate its privileges by modifying system files without user's knowledge. Successful exploitation requires uncommon system configuration.	gvfs	Unchanged	Not vulnerable	Not vulnerable	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3792
457	CVE-2019-3825	Medium	MEDIUM	A vulnerability was discovered in gdm before 3.31.4. When timed login is enabled in configuration, an attacker could bypass the lock screen by selecting the timed login user and waiting for the timer to expire, at which time they would gain access to the logged-in user's session.	gdm	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-8067
458	CVE-2019-3824	Medium	MEDIUM	A flaw was found in the way an LDAP search expression could crash the shared LDAP server process of a samba AD DC in samba before version 4.10. An authenticated user, having read permissions on the LDAP server, could use this flaw to cause denial of service.	samba	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3780
459	CVE-2019-3823	High	CRITICAL	libcurl versions from 7.34.0 to before 7.64.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-response for SMTP. If the buffer passed to `smtp_endofresp()` isn't NUL terminated and contains no character ending the parsed number, and `len` is set to 5, then the `strtol()` call reads beyond the allocated buffer. The read contents will not be returned to the caller.	curl	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3552
460	CVE-2019-3822	HIGH	CRITICAL	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.	curl	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3596

	A	B	C	D	E	F	G	H	I	J	K	L	M
461	CVE-2019-3821	MEDIUM	HIGH	A flaw was found in the way civetweb frontend was handling requests for ceph RGW server with SSL enabled. An unauthenticated attacker could create multiple connections to ceph RADOS gateway to exhaust file descriptors for ceph-radosgw service resulting in a remote denial of service.	ceph	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3807
462	CVE-2019-3819	Medium	MEDIUM	A flaw was found in the Linux kernel in the function hid_debug_events_read() in drivers/hid/hid-debug.c file which may enter an infinite loop with certain parameters passed from a userspace. A local privileged user (root) can cause a system lock up and a denial of service. Versions from v4.18 and newer are vulnerable.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3519
463	CVE-2019-3817	Medium	HIGH	A use-after-free flaw has been discovered in libcomps before version 0.1.10 in the way ObjMRTrees are merged. An attacker, who is able to make an application read a crafted comps XML file, may be able to crash the application or execute malicious code.	libcomps	Unchanged	Not vulnerable	Not vulnerable	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3808
464	CVE-2019-3816	Medium	HIGH	Openwsman, versions up to and including 2.6.9, are vulnerable to arbitrary file disclosure because the working directory of openwsmand daemon was set to root directory. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to openwsman server.	openwsman	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3777
465	CVE-2019-3815	Low	LOW	A memory leak was discovered in the backport of fixes for CVE-2018-16864 in Red Hat Enterprise Linux. Function dispatch_message_real() in journald-server.c does not free the memory allocated by set_iovec_field_free() to store the `_CMDLINE=` entry. A local attacker may use this flaw to make systemd-journald crash. This issue only affects versions shipped with Red Hat Enterprise since v219-62.2.	systemd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3533
466	CVE-2019-3814	Medium	MEDIUM	It was discovered that Dovecot before versions 2.2.36.1 and 2.3.4.1 incorrectly handled client certificates. A remote attacker in possession of a valid certificate with an empty username field could possibly use this issue to impersonate other users.	dovecot	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-3811
467	CVE-2019-3813	Medium	HIGH	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers.	spice	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	10.19.45.1	Not vulnerable	LIN1018-3567
468	CVE-2019-3812	Low	MEDIUM	QEMU, through version 2.10 and through version 3.1.0, is vulnerable to an out-of-bounds read of up to 128 bytes in the hw/i2c/i2c-ddc.c:i2c_ddc() function. A local attacker with permission to execute i2c commands could exploit this to read stack memory of the qemu process on the host.	qemu	Unchanged	Not vulnerable	9.0.0.21	10.17.41.15	10.18.44.5	10.19.45.1	Not vulnerable	LIN1018-3651
469	CVE-2019-3811	LOW	MEDIUM	An issue was found in SSSD. The default option for fallback_homedir returns '/' for empty home directories in the passwd file.	sssd	Unchanged	Not vulnerable	Won't Fix	Won't Fix	10.18.44.15	Not vulnerable	Not vulnerable	LIN1018-3417
470	CVE-2019-3805	Medium	MEDIUM	A flaw was discovered in wildfly versions up to 16.0.0.Final that would allow local users who are able to execute init.d script to terminate arbitrary processes on the system. An attacker could exploit this by modifying the PID file in /var/run/jboss-eap/ allowing the init.d script to terminate any process as root.	wildfly	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10880
471	CVE-2019-3701	HIGH	MEDIUM	An issue was discovered in can_can_gw_rcv in net/can/gw.c in the Linux kernel through 4.19.13. The CAN frame modification rules allow bitwise logical operations that can be also applied to the can_dlc field. Because of a missing check, the CAN drivers may write arbitrary content beyond the data registers in the CAN controller's I/O memory when processing can-gw manipulated outgoing frames. This is related to cgw_csum_xor_rel. An unprivileged user can trigger a system crash (general protection fault).	linux	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3399
472	CVE-2019-3462	HIGH	HIGH	Incorrect sanitation of the 302 redirect field in HTTP transport method of apt versions 1.4.8 and earlier can lead to content injection by a MITM attacker, potentially leading to remote code execution on the target machine.	apt	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	Investigate	Not vulnerable	LIN1018-3584
473	CVE-2019-3460	LOW	MEDIUM	A flaw was found in the Linux kernels implementation of Logical link control and adaptation protocol (L2CAP), part of the bluetooth stack in the l2cap_parse_conf_rsp, l2cap_parse_conf_req functions.	linux	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3387
474	CVE-2019-3459	LOW	MEDIUM	A flaw was found in the Linux kernels implementation of Logical link control and adaptation protocol (L2CAP), part of the bluetooth stack.	linux	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3400
475	CVE-2019-3018	LOW	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5133
476	CVE-2019-3016	LOW	MEDIUM	In a Linux KVM guest that has PV TLB enabled, a process in the guest kernel may be able to read memory locations from another process in the same guest. This problem is limit to the host running linux kernel 4.10 with a guest running linux kernel 4.16 or later. The problem mainly affects AMD processors but Intel CPUs cannot be ruled out.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.20	10.18.44.15	Investigate	Investigate	LIN1019-4048

	A	B	C	D	E	F	G	H	I	J	K	L	M
477	CVE-2019-3011	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: C API). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5134
478	CVE-2019-3009	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection). Supported versions that are affected are 8.0.17 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5135
479	CVE-2019-3004	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5136
480	CVE-2019-3003	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5137
481	CVE-2019-2999	MEDIUM	MEDIUM	Vulnerability in the Java SE product of Oracle Java SE (component: Javadoc). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11661
482	CVE-2019-2998	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5138
483	CVE-2019-2997	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1018-5139

	A	B	C	D	E	F	G	H	I	J	K	L	M
484	CVE-2019-2996	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u221; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11662
485	CVE-2019-2993	LOW	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: C API). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5140
486	CVE-2019-2992	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11663
487	CVE-2019-2991	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.017 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5141
488	CVE-2019-2988	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11664

	A	B	C	D	E	F	G	H	I	J	K	L	M
489	CVE-2019-2987	MEDIUM	LOW	Vulnerability in the Java SE product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11665
490	CVE-2019-2983	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11630
491	CVE-2019-2982	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5114
492	CVE-2019-2981	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11631
493	CVE-2019-2978	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11632

	A	B	C	D	E	F	G	H	I	J	K	L	M
494	CVE-2019-2977	MEDIUM	MEDIUM	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.8 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11633
495	CVE-2019-2975	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11634
496	CVE-2019-2974	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.45 and prior, 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.6	Not vulnerable	LIN1018-5115
497	CVE-2019-2973	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11635
498	CVE-2019-2969	LOW	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 6.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	mysql	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-5116
499	CVE-2019-2968	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5117

	A	B	C	D	E	F	G	H	I	J	K	L	M
500	CVE-2019-2967	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5118
501	CVE-2019-2966	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5119
502	CVE-2019-2964	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11636
503	CVE-2019-2963	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5120
504	CVE-2019-2962	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11637
505	CVE-2019-2960	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5121
506	CVE-2019-2958	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11638

	A	B	C	D	E	F	G	H	I	J	K	L	M
507	CVE-2019-2957	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5122
508	CVE-2019-2950	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5123
509	CVE-2019-2949	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11639
510	CVE-2019-2948	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5124
511	CVE-2019-2946	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5125
512	CVE-2019-2945	LOW	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11640
513	CVE-2019-2938	LOW	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.6	Not vulnerable	LIN1018-5126

	A	B	C	D	E	F	G	H	I	J	K	L	M
514	CVE-2019-2933	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11641
515	CVE-2019-2924	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-5127
516	CVE-2019-2923	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-5128
517	CVE-2019-2922	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-5129
518	CVE-2019-2920	MEDIUM	MEDIUM	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/ODBC). Supported versions that are affected are 5.3.13 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	mysql	Unchanged	Vulnerable	Vulnerable	Investigate	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-5130
519	CVE-2019-2914	MEDIUM	MEDIUM	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5131
520	CVE-2019-2911	MEDIUM	LOW	Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.6.45 and prior, 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-5187

	A	B	C	D	E	F	G	H	I	J	K	L	M
521	CVE-2019-2910	MEDIUM	LOW	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 5.6.45 and prior and 5.7.27 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-5132
522	CVE-2019-2879	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4486
523	CVE-2019-2842	Medium	LOW	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JCE). The supported version that is affected is Java SE: 8u212. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11200
524	CVE-2019-2834	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4487
525	CVE-2019-2830	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4488
526	CVE-2019-2826	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4489
527	CVE-2019-2822	Medium	HIGH	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell: Admin / InnoDB Cluster). Supported versions that are affected are 8.0.16 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4490

	A	B	C	D	E	F	G	H	I	J	K	L	M
528	CVE-2019-2821	Low	MEDIUM	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11209
529	CVE-2019-2819	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4491
530	CVE-2019-2818	Low	LOW	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11207
531	CVE-2019-2816	Medium	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11208
532	CVE-2019-2815	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4492
533	CVE-2019-2814	Low	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.2 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4493

	A	B	C	D	E	F	G	H	I	J	K	L	M
534	CVE-2019-2812	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4494
535	CVE-2019-2811	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4495
536	CVE-2019-2810	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4496
537	CVE-2019-2808	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4497
538	CVE-2019-2805	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.6	Not vulnerable	LIN1018-4498
539	CVE-2019-2803	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4499
540	CVE-2019-2802	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4500
541	CVE-2019-2801	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4501

	A	B	C	D	E	F	G	H	I	J	K	L	M
542	CVE-2019-2800	Medium	HIGH	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4502
543	CVE-2019-2798	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4503
544	CVE-2019-2797	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4504
545	CVE-2019-2796	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4505
546	CVE-2019-2795	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4506
547	CVE-2019-2791	Medium	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4507
548	CVE-2019-2789	Medium	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4508

	A	B	C	D	E	F	G	H	I	J	K	L	M
549	CVE-2019-2786	Low	LOW	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11233
550	CVE-2019-2785	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4509
551	CVE-2019-2784	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4510
552	CVE-2019-2780	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Components / Services). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4511
553	CVE-2019-2778	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4512
554	CVE-2019-2774	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4513

	A	B	C	D	E	F	G	H	I	J	K	L	M
555	CVE-2019-2769	Medium	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11234
556	CVE-2019-2766	Low	LOW	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11235
557	CVE-2019-2762	Medium	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11236
558	CVE-2019-2758	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.6	Not vulnerable	LIN1018-4515
559	CVE-2019-2757	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4516
560	CVE-2019-2755	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4517

	A	B	C	D	E	F	G	H	I	J	K	L	M
561	CVE-2019-2752	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4518
562	CVE-2019-2747	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4519
563	CVE-2019-2746	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Data Dictionary). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4520
564	CVE-2019-2745	Low	MEDIUM	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 7u221, 8u212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11251
565	CVE-2019-2743	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.12 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4521
566	CVE-2019-2741	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Log). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4522
567	CVE-2019-2740	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.6	Not vulnerable	LIN1018-4523

	A	B	C	D	E	F	G	H	I	J	K	L	M
568	CVE-2019-2739	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.6	Not vulnerable	LIN1018-4524
569	CVE-2019-2738	Low	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Compiling). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4525
570	CVE-2019-2737	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.6	Not vulnerable	LIN1018-4526
571	CVE-2019-2731	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4527
572	CVE-2019-2730	Medium	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.44 and prior and 5.7.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4528
573	CVE-2019-2698	Medium	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10859
574	CVE-2019-2697	Medium	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10860

	A	B	C	D	E	F	G	H	I	J	K	L	M
575	CVE-2019-2695	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3989
576	CVE-2019-2694	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3979
577	CVE-2019-2693	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3980
578	CVE-2019-2692	Low	MEDIUM	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Connectors executes to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3981
579	CVE-2019-2691	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3982
580	CVE-2019-2689	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3983
581	CVE-2019-2688	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3984
582	CVE-2019-2687	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3985

	A	B	C	D	E	F	G	H	I	J	K	L	M
583	CVE-2019-2686	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3986
584	CVE-2019-2685	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3987
585	CVE-2019-2684	Medium	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10861
586	CVE-2019-2683	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3990
587	CVE-2019-2681	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3991
588	CVE-2019-2644	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3992
589	CVE-2019-2636	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Group Replication Plugin). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via MySQL Procotol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4017

	A	B	C	D	E	F	G	H	I	J	K	L	M
590	CVE-2019-2635	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3993
591	CVE-2019-2634	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3994
592	CVE-2019-2632	Medium	HIGH	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3995
593	CVE-2019-2631	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Information Schema). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3996
594	CVE-2019-2630	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3997
595	CVE-2019-2628	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: innoDB). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3998
596	CVE-2019-2627	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4018
597	CVE-2019-2626	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3999

	A	B	C	D	E	F	G	H	I	J	K	L	M
598	CVE-2019-2625	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4000
599	CVE-2019-2624	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4001
600	CVE-2019-2623	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4002
601	CVE-2019-2620	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4019
602	CVE-2019-2617	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4003
603	CVE-2019-2614	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4004
604	CVE-2019-2607	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4005
605	CVE-2019-2606	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4006

	A	B	C	D	E	F	G	H	I	J	K	L	M
606	CVE-2019-2602	Medium	HIGH	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10862
607	CVE-2019-2596	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4007
608	CVE-2019-2593	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4008
609	CVE-2019-2592	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4009
610	CVE-2019-2589	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4010
611	CVE-2019-2587	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4011
612	CVE-2019-2585	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4012
613	CVE-2019-2584	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4013

	A	B	C	D	E	F	G	H	I	J	K	L	M
614	CVE-2019-2581	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4014
615	CVE-2019-2580	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4020
616	CVE-2019-2566	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4021
617	CVE-2019-2540	Medium	MEDIUM	Vulnerability in the Java Advanced Management Console component of Oracle Java SE (subcomponent: Server). The supported version that is affected is Java Advanced Management Console: 2.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java Advanced Management Console. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java Advanced Management Console, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java Advanced Management Console accessible data as well as unauthorized read access to a subset of Java Advanced Management Console accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10487
618	CVE-2019-2539	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3573
619	CVE-2019-2537	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3532
620	CVE-2019-2536	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3514

	A	B	C	D	E	F	G	H	I	J	K	L	M
621	CVE-2019-2535	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3566
622	CVE-2019-2534	Medium	HIGH	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3506
623	CVE-2019-2533	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3593
624	CVE-2019-2532	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3581
625	CVE-2019-2531	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3498
626	CVE-2019-2530	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3557
627	CVE-2019-2529	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-3515
628	CVE-2019-2528	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3549

	A	B	C	D	E	F	G	H	I	J	K	L	M
629	CVE-2019-2513	Low	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3511
630	CVE-2019-2510	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3579
631	CVE-2019-2507	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3540
632	CVE-2019-2503	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection Handling). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3503
633	CVE-2019-2502	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3583
634	CVE-2019-2495	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3556
635	CVE-2019-2494	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3590
636	CVE-2019-2486	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3504

	A	B	C	D	E	F	G	H	I	J	K	L	M
637	CVE-2019-2482	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3516
638	CVE-2019-2481	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3577
639	CVE-2019-2455	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3508
640	CVE-2019-2449	Low	LOW	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). The supported version that is affected is Java SE: 8u192. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10508
641	CVE-2019-2436	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3497
642	CVE-2019-2435	Medium	HIGH	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/Python). Supported versions that are affected are 8.0.13 and prior and 2.1.8 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Connectors accessible data as well as unauthorized access to critical data or complete access to all MySQL Connectors accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3571
643	CVE-2019-2434	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3564

	A	B	C	D	E	F	G	H	I	J	K	L	M
644	CVE-2019-2426	Medium	LOW	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u201, 8u192 and 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10499
645	CVE-2019-2422	Medium	LOW	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u201, 8u192 and 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10478
646	CVE-2019-2420	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3542
647	CVE-2019-2389	Low	MEDIUM	Incorrect scoping of kill operations in MongoDB Server's packaged SysV init scripts allow users with write access to the PID file to insert arbitrary PIDs to be killed when the root user stops the MongoDB process via SysV init. This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.11; v3.6 versions prior to 3.6.14; v3.4 versions prior to 3.4.22.	mongodb	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4813
648	CVE-2019-2386	MEDIUM	HIGH	After user deletion in MongoDB Server the improper invalidation of authorization sessions allows an authenticated user's session to persist and become conflated with new accounts, if those accounts reuse the names of deleted ones. This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.9; v3.6 versions prior to 3.6.13; v3.4 versions prior to 3.4.22.	mongodb	Unchanged	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4625
649	CVE-2019-20636	HIGH	CRITICAL	In the Linux kernel before 5.4.12, drivers/input/input.c has out-of-bounds writes via a crafted keycode table, as demonstrated by input_set_keycode, aka CID-cb222aed03d7.	linux	New	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4263
650	CVE-2019-20633	MEDIUM	MEDIUM	GNU patch through 2.7.6 contains a free(p_line[p_end]) Double Free vulnerability in the function another_hunk in pch.c that can cause a denial of service via a crafted patch file. NOTE: this issue exists because of an incomplete fix for CVE-2018-6952.	patch	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4184
651	CVE-2019-20503	MEDIUM	MEDIUM	usrsctp before 2019-12-20 has out-of-bounds reads in sctp_load_addresses_from_init.	usrsctp	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4119
652	CVE-2019-20485	LOW	MEDIUM	qemu/qemu_driver.c in libvirt before 6.0.0 mishandles the holding of a monitor job during a query to a guest agent, which allows attackers to cause a denial of service (API blockage).	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.6	Not vulnerable	LIN1019-4155
653	CVE-2019-20477	HIGH	CRITICAL	PyYAML 5.1 through 5.1.2 has insufficient restrictions on the load and load_all functions because of a class deserialization issue, e.g., Popen is a class in the subprocess module. NOTE: this issue exists because of an incomplete fix for CVE-2017-18342.	python-pyyaml	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4064
654	CVE-2019-20454	MEDIUM	HIGH	An out-of-bounds read was discovered in PCRE before 10.34 when the pattern \X is JIT compiled and used to match specially crafted subjects in non-UTF mode. Applications that use PCRE to parse untrusted input may be vulnerable to this flaw, which would allow an attacker to crash the application. The flaw occurs in do_extuni_no_utf in pcre2_jit_compile.c.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.15	10.19.45.5	Not vulnerable	LIN1019-4063
655	CVE-2019-20446	MEDIUM	MEDIUM	In xml.rs in GNOME librsvg before 2.46.2, a crafted SVG file with nested patterns can cause denial of service when passed to the library for processing. The attacker constructs pattern elements so that the number of final rendered objects grows exponentially.	librsvg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1019-4003
656	CVE-2019-20433	MEDIUM	CRITICAL	libaspell.a in GNU Aspell before 0.60.8 has a buffer over-read for a string ending with a single '0' byte, if the encoding is set to ucs-2 or ucs-4 outside of the application, as demonstrated by the ASPELL_CONF environment variable.	aspell	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.6	Not vulnerable	LIN1019-3983

	A	B	C	D	E	F	G	H	I	J	K	L	M
657	CVE-2019-20422	LOW	MEDIUM	In the Linux kernel before 5.3.4, fib6_rule_lookup in net/ipv6/ip6_fib.c mishandles the RT6_LOOKUP_F_DST_NOREF flag in a reference-count decision, leading to (for example) a crash that was identified by syzkaller, aka CID-7b09c2d052db.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3984
658	CVE-2019-20388	MEDIUM	HIGH	xmlSchemaPreRun in xmlschemas.c in libxml2 2.9.10 allows an xmlSchemaValidateStream memory leak.	libxml2	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.5	10.20.9.0	LIN1019-3965
659	CVE-2019-20387	MEDIUM	HIGH	repodata_schema2id in repodata.c in libsolv before 0.7.6 has a heap-based buffer over-read via a last schema whose length is less than the length of the input schema.	libsolv	Unchanged	Not vulnerable	9.0.0.25	10.17.41.20	10.18.44.14	Not vulnerable	Not vulnerable	LIN1019-3968
660	CVE-2019-20386	LOW	LOW	An issue was discovered in button_open in login/logind-button.c in systemd before 243. When executing the udevadm trigger command, a memory leak may occur.	systemd	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	Not vulnerable	Not vulnerable	LIN1019-3967
661	CVE-2019-20382	MEDIUM	MEDIUM	QEMU 4.1.0 has a memory leak in zrle_compress_data in ui/vnc-enc-zrle.c during a VNC disconnect operation because libz is misused, resulting in a situation where memory allocated in deflateInit2 is not freed in deflateEnd.	qemu	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.6	10.20.12.0	LIN1019-4116
662	CVE-2019-20372	MEDIUM	MEDIUM	NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.	nginx	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	10.18.44.15	10.19.45.6	Won't Fix	LIN1019-3910
663	CVE-2019-20367	MEDIUM	CRITICAL	nlist.c in libbsd before 0.10.0 has an out-of-bounds read during a comparison for a symbol name from the string table (strtab).	libbsd	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN1019-3902
664	CVE-2019-20352	MEDIUM	HIGH	In Netwide Assembler (NASM) 2.15rc0, a heap-based buffer over-read occurs (via a crafted .asm file) in set_text_free when called from expand_one_smacro in asm/preproc.c.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1019-3891
665	CVE-2019-20334	MEDIUM	MEDIUM	In Netwide Assembler (NASM) 2.14.02, stack consumption occurs in expr# functions in asm/eval.c. This potentially affects the relationships among expr0, expr1, expr2, expr3, expr4, expr5, and expr6 (and stdscan in asm/stdscan.c). This is similar to CVE-2019-6290 and CVE-2019-6291.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1019-3887
666	CVE-2019-20326	MEDIUM	HIGH	A heap-based buffer overflow in _cairo_image_surface_create_from_jpeg( ) in extensions/cairo_io/cairo-image-surface-jpeg.c in GNOME gThumb before 3.8.3 and Linux Mint Pix before 2.4.5 allows attackers to cause a crash and potentially execute arbitrary code via a crafted JPEG file.	gthumb	Unchanged	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-9699
667	CVE-2019-20218	MEDIUM	HIGH	selectExpander in select.c in SQLite 3.30.1 proceeds with WITH stack unwinding even after a parsing error.	sqlite	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.3	10.20.6.0	LIN1019-3882
668	CVE-2019-20176	MEDIUM	HIGH	In Pure-FTPd 1.0.49, a stack exhaustion issue was discovered in the listdir function in ls.c.	pure-ftpd	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3916
669	CVE-2019-20175	MEDIUM	HIGH	** DISPUTED ** An issue was discovered in ide_dma_cb() in hw/ide/core.c in QEMU 2.4.0 through 4.2.0. The guest system can crash the QEMU process in the host system via a special SCSI_IOCTL_SEND_COMMAND. It hits an assertion that implies that the size of successful DMA transfers there must be a multiple of 512 (the size of a sector). NOTE: a member of the QEMU security team disputes the significance of this issue because a privileged guest user has many ways to cause similar DoS effect, without triggering this assert.	qemu	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.16	10.19.45.6	Investigate	LIN1019-3886
670	CVE-2019-20096	MEDIUM	MEDIUM	In the Linux kernel before 5.1, there is a memory leak in __feat_register_sp() in net/dccp/feat.c, which may cause denial of service, aka CID-1d3ff0950e2b.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	Not vulnerable	Not vulnerable	LIN1019-3869
671	CVE-2019-20095	MEDIUM	MEDIUM	mwifiex_tm_cmd in drivers/net/wireless/marvell/mwifiex/cfg80211.c in the Linux kernel before 5.1.6 has some error-handling cases that did not free allocated hostcmd memory, aka CID-003b686ace82. This will cause a memory leak and denial of service.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.20	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3870
672	CVE-2019-20079	HIGH	CRITICAL	The autocmd feature in window.c in Vim before 8.1.2136 accesses freed memory.	vim	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3871
673	CVE-2019-20054	MEDIUM	MEDIUM	In the Linux kernel before 5.0.6, there is a NULL pointer dereference in drop_sysctl_table() in fs/proc/proc_sysctl.c, related to put_links, aka CID-23da9588037e.	linux	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN1019-3872
674	CVE-2019-20044	HIGH	HIGH	In Zsh before 5.8, attackers able to execute commands can regain privileges dropped by the --no-PRIVILEGED option. Zsh fails to overwrite the saved uid, so the original privileges can be restored by executing MODULE_PATH=/dir/with/module zmodload with a module that calls setuid().	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4074
675	CVE-2019-19977	HIGH	CRITICAL	libESMTP through 1.0.6 mishandles domain copying into a fixed-size buffer in ntlm_build_type_2 in ntlm/ntlmstruct.c, as demonstrated by a stack-based buffer over-read.	libesmtp	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3863
676	CVE-2019-19966	LOW	MEDIUM	In the Linux kernel before 5.1.6, there is a use-after-free in cpia2_exit() in drivers/media/usb/cpia2/cpia2_v4l.c that will cause denial of service, aka CID-dea37a972655.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3850
677	CVE-2019-19965	LOW	MEDIUM	In the Linux kernel through 5.4.6, there is a NULL pointer dereference in drivers/scsi/libsas/sas_discover.c because of mishandling of port disconnection during discovery, related to a PHY down race condition, aka CID-f70267f379b5.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3851
678	CVE-2019-19963	MEDIUM	MEDIUM	An issue was discovered in wolfSSL before 4.3.0 in a non-default configuration where DSA is enabled. DSA signing uses the BEEA algorithm during modular inversion of the nonce, leading to a side-channel attack against the nonce.	wolfssl	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3852
679	CVE-2019-19962	MEDIUM	HIGH	wolfSSL before 4.3.0 mishandles calls to wc_SignatureGenerateHash, leading to fault injection in RSA cryptography.	wolfssl	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3853
680	CVE-2019-19960	MEDIUM	MEDIUM	In wolfSSL before 4.3.0, wc_ecc_mulmod_ex does not properly resist side-channel attacks.	wolfssl	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3854

	A	B	C	D	E	F	G	H	I	J	K	L	M
681	CVE-2019-19959	MEDIUM	HIGH	ext/misc/zipfile.c in SQLite 3.30.1 mishandles certain uses of INSERT INTO in situations involving embedded '\0' characters in filenames, leading to a memory-management error that can be detected by (for example) valgrind.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.3	10.20.6.0	LIN1019-3883
682	CVE-2019-19956	MEDIUM	HIGH	xmlParseBalancedChunkMemoryRecover in parser.c in libxml2 before 2.9.10 has a memory leak related to newDoc->oldNs.	libxml2	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3862
683	CVE-2019-19952	HIGH	CRITICAL	In ImageMagick 7.0.9-7 Q16, there is a use-after-free in the function MngInfoDiscardObject of coders/png.c, related to ReadOneMNGImage.	imagemagick	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3838
684	CVE-2019-19949	MEDIUM	CRITICAL	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer over-read in the function WritePNGImage of coders/png.c, related to Magick_png_write_raw_profile and LocaleNCompare.	imagemagick	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3839
685	CVE-2019-19948	HIGH	CRITICAL	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer overflow in the function WriteSGIImage of coders/sgi.c.	imagemagick	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3840
686	CVE-2019-19947	LOW	MEDIUM	In the Linux kernel through 5.4.6, there are information leaks of uninitialized memory to a USB device in the drivers/net/can/usb/kvaser_usb/kvaser_usb_leaf.c driver, aka CID-da2311a6385c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.4	Not vulnerable	LIN1019-3841
687	CVE-2019-19927	LOW	HIGH	In the Linux kernel 5.0.0-rc7 (as distributed in ubuntu/linux.git on kernel.ubuntu.com), mounting a crafted f2fs filesystem image and performing some operations can lead to slab-out-of-bounds read access in ttm_put_pages in drivers/gpu/drm/ttm/ttm_page_alloc.c. This is related to the vmwgfx or ttm module.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	Not vulnerable	Not vulnerable	LIN1019-3881
688	CVE-2019-19926	MEDIUM	HIGH	multiSelect in select.c in SQLite 3.30.1 mishandles certain errors during parsing, as demonstrated by errors from sqlite3WindowRewrite() calls. NOTE: this vulnerability exists because of an incomplete fix for CVE-2019-19880.	sqlite	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.3	10.20.6.0	LIN1019-3825
689	CVE-2019-19925	MEDIUM	HIGH	zipfileUpdate in ext/misc/zipfile.c in SQLite 3.30.1 mishandles a NULL pathname during an update of a ZIP archive.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.3	10.20.6.0	LIN1019-3855
690	CVE-2019-19924	MEDIUM	MEDIUM	SQLite 3.30.1 mishandles certain parser-tree rewriting, related to expr.c, vdbeaux.c, and window.c. This is caused by incorrect sqlite3WindowRewrite() error handling.	sqlite	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.3	10.20.6.0	LIN1019-3856
691	CVE-2019-19923	MEDIUM	HIGH	flattenSubquery in select.c in SQLite 3.30.1 mishandles certain uses of SELECT DISTINCT involving a LEFT JOIN in which the right-hand side is a view. This can cause a NULL pointer dereference (or incorrect results).	sqlite	Unchanged	Not vulnerable	Not vulnerable	10.17.41.20	10.18.44.14	10.19.45.3	10.20.6.0	LIN1019-3857
692	CVE-2019-19922	LOW	MEDIUM	kernel/sched/fair.c in the Linux kernel before 5.3.9, when cpu.cfs_quota_us is used (e.g., with Kubernetes), allows attackers to cause a denial of service against non-cpu-bound applications by generating a workload that triggers unwanted slice expiration, aka CID-de53fd7aedb1. (In other words, although this slice expiration would typically be seen with benign workloads, it is possible that an attacker could calculate how many stray requests are required to force an entire Kubernetes cluster into a low-performance state caused by slice expiration, and ensure that a DDoS attack sent that number of stray requests. An attack does not affect the stability of the kernel; it only causes mismanagement of application execution.)	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	10.19.45.3	Not vulnerable	LIN1019-3826
693	CVE-2019-19921	MEDIUM	HIGH	runc through 1.0.0-rc9 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. (This vulnerability does not affect Docker due to an implementation detail that happens to block the attack.)	runc-opencontainers	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4041
694	CVE-2019-19906	MEDIUM	HIGH	cyrus-sasl (aka Cyrus SASL) 2.1.27 has an out-of-bounds write leading to unauthenticated remote denial-of-service in OpenLDAP via a malformed LDAP packet. The OpenLDAP crash is ultimately caused by an off-by-one error in _sasl_add_string in common.c in cyrus-sasl.	cyrus-sasl	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.5	10.20.12.0	LIN1019-3823
695	CVE-2019-19882	MEDIUM	HIGH	shadow 4.8, in certain circumstances affecting at least Gentoo, Arch Linux, and Void Linux, allows local users to obtain root access because setuid programs are misconfigured. Specifically, this affects shadow 4.8 when compiled using --with-libpam but without explicitly passing --disable-account-tools-setuid, and without a PAM configuration suitable for use with setuid account management tools. This combination leads to account management tools (groupadd, groupdel, groupmod, useradd, userdel, usermod) that can easily be used by unprivileged local users to escalate privileges to root in multiple ways. This issue became much more relevant in approximately December 2019 when an unrelated bug was fixed (i.e., the chmod calls to suidusbins were fixed in the upstream Makefile which is now included in the release version 4.8).	shadow	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.3	10.20.3.0	LIN1019-3811
696	CVE-2019-19880	MEDIUM	HIGH	exprListAppendList in window.c in SQLite 3.30.1 allows attackers to trigger an invalid pointer dereference because constant integer values in ORDER BY clauses of window definitions are mishandled.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.3	10.20.6.0	LIN1019-3812
697	CVE-2019-19816	HIGH	HIGH	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3797
698	CVE-2019-19815	HIGH	MEDIUM	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause a NULL pointer dereference in f2fs_recover_fsync_data in fs/f2fs/recovery.c. This is related to F2FS_P_SB in fs/f2fs/f2fs.h.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3798

	A	B	C	D	E	F	G	H	I	J	K	L	M
699	CVE-2019-19814	HIGH	HIGH	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of dirty types (8) but the array index can exceed this.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3799
700	CVE-2019-19813	HIGH	HIGH	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image, performing some operations, and then making a syncfs system call can lead to a use-after-free in __mutex_lock in kernel/locking/mutex.c. This is related to mutex_can_spin_on_owner in kernel/locking/mutex.c, __btrfs_qgroup_free_meta in fs/btrfs/qgroup.c, and btrfs_insert_delayed_items in fs/btrfs/delayed-inode.c.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3800
701	CVE-2019-19807	MEDIUM	MEDIUM	In the Linux kernel before 5.3.11, sound/core/timer.c has a use-after-free caused by erroneous code refactoring, aka CID-e7af6307a8a5. This is related to snd_timer_open and snd_timer_close_locked. The timeri variable was originally intended to be for a newly created timer instance, but was used for a different purpose after refactoring.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.4	Not vulnerable	LIN1019-3789
702	CVE-2019-19770	MEDIUM	HIGH	In the Linux kernel 4.19.83, there is a use-after-free (read) in the debugfs_remove function in fs/debugfs/inode.c (which is used to remove a file or directory in debugfs that was previously created with a call to another debugfs function such as debugfs_create_file).	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1019-3774
703	CVE-2019-19769	MEDIUM	HIGH	In the Linux kernel 5.3.10, there is a use-after-free (read) in the perf_trace_lock_acquire function (related to include/trace/events/lock.h).	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.7	Not vulnerable	LIN1019-3775
704	CVE-2019-19768	MEDIUM	HIGH	In the Linux kernel 5.4.0-rc2, there is a use-after-free (read) in the __blk_add_trace function in kernel/trace/blktrace.c (which is used to fill out a blk_io_trace structure and place it in a per-cpu sub-buffer).	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1019-3776
705	CVE-2019-19767	MEDIUM	MEDIUM	The Linux kernel before 5.4.2 mishandles ext4_expand_extra_isize, as demonstrated by use-after-free errors in __ext4_expand_extra_isize and ext4_xattr_set_entry, related to fs/ext4/inode.c and fs/ext4/super.c, aka CID-4ea99936a163.	linux	Unchanged	Investigate	Investigate	10.17.41.20	10.18.44.15	10.19.45.3	Not vulnerable	LIN1019-3777
706	CVE-2019-19725	HIGH	CRITICAL	sysstat through 12.2.0 has a double free in check_file_actlst in sa_common.c.	sysstat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3769
707	CVE-2019-19722	MEDIUM	MEDIUM	In Dovecot before 2.3.9.2, an attacker can crash a push-notification driver with a crafted email when push notifications are used, because of a NULL Pointer Dereference. The email must use a group address as either the sender or the recipient.	dovecot	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3778
708	CVE-2019-19646	HIGH	CRITICAL	pragma.c in SQLite through 3.30.1 mishandles NOT NULL in an integrity_check PRAGMA command in certain cases of generated columns.	sqlite	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3735
709	CVE-2019-19645	LOW	MEDIUM	alter.c in SQLite through 3.30.1 allows attackers to trigger infinite recursion via certain types of self-referential views in conjunction with ALTER TABLE statements.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.3	Not vulnerable	LIN1019-3736
710	CVE-2019-19624	MEDIUM	MEDIUM	An out-of-bounds read was discovered in OpenCV before 4.1.1. Specifically, variable coarsest_scale is assumed to be greater than or equal to finest_scale within the calc()/ocl_calc() functions in dis_flow.cpp. However, this is not true when dealing with small images, leading to an out-of-bounds read of the heap-allocated arrays Ux and Uy.	opencv	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3724
711	CVE-2019-19617	HIGH	CRITICAL	phpMyAdmin before 4.9.2 does not escape certain Git information, related to libraries/classes/Display/GitRevision.php and libraries/classes/Footer.php.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	Investigate	Not vulnerable	LIN1019-3716
712	CVE-2019-19604	HIGH	CRITICAL	Arbitrary command execution is possible in Git before 2.20.2, 2.21.x before 2.21.1, 2.22.x before 2.22.2, 2.23.x before 2.23.1, and 2.24.x before 2.24.1 because a git submodule update operation can run commands found in the .gitmodules file of a malicious repository.	git	Unchanged	Investigate	Investigate	Investigate	Investigate	10.19.45.6	Not vulnerable	LIN1019-3748
713	CVE-2019-19603	HIGH	CRITICAL	SQLite 3.30.1 mishandles certain SELECT statements with a nonexistent VIEW, leading to an application crash.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.3	Not vulnerable	LIN1019-3737
714	CVE-2019-19602	MEDIUM	HIGH	fpregs_state_valid in arch/x86/include/asm/fpu/internal.h in the Linux kernel before 5.4.2, when GCC 9 is used, allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact because of incorrect fpu_fpregs_owner_ctx caching, as demonstrated by mishandling of signal-based non-cooperative preemption in Go 1.14 prereleases on amd64, aka CID-59c4bd853abc.	linux	Unchanged	Not vulnerable	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3717
715	CVE-2019-19553	MEDIUM	HIGH	In Wireshark 3.0.0 to 3.0.6 and 2.6.0 to 2.6.12, the CMS dissector could crash. This was addressed in epan/dissectors/asn1/cms/packet-cms-template.c by ensuring that an object identifier is set to NULL after a ContentInfo dissection.	wireshark	Unchanged	Not vulnerable	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Investigate	LIN1019-3712
716	CVE-2019-19543	MEDIUM	HIGH	In the Linux kernel before 5.1.6, there is a use-after-free in serial_ir_init_module() in drivers/media/rc/serial_ir.c.	linux	Unchanged	Not vulnerable	Vulnerable	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3684
717	CVE-2019-19537	MEDIUM	MEDIUM	In the Linux kernel before 5.2.10, there is a race condition bug that can be caused by a malicious USB device in the USB character device driver layer, aka CID-303911cfc5b9. This affects drivers/usb/core/file.c.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3685
718	CVE-2019-19536	LOW	MEDIUM	In the Linux kernel before 5.2.9, there is an info-leak bug that can be caused by a malicious USB device in the drivers/net/can/usb/peak_usb/pcan_usb_pro.c driver, aka CID-ead16e53c2f0.	linux	Unchanged	Investigate	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3686
719	CVE-2019-19535	LOW	MEDIUM	In the Linux kernel before 5.2.9, there is an info-leak bug that can be caused by a malicious USB device in the drivers/net/can/usb/peak_usb/pcan_usb_fd.c driver, aka CID-30a8beeb3042.	linux	Unchanged	8.0.0.32	9.0.0.24	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3687
720	CVE-2019-19534	LOW	LOW	In the Linux kernel before 5.3.11, there is an info-leak bug that can be caused by a malicious USB device in the drivers/net/can/usb/peak_usb/pcan_usb_core.c driver, aka CID-f7a1337f0d29.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	10.20.3.0	LIN1019-3688

	A	B	C	D	E	F	G	H	I	J	K	L	M
721	CVE-2019-19533	LOW	LOW	In the Linux kernel before 5.3.4, there is an info-leak bug that can be caused by a malicious USB device in the drivers/media/usb/ttusb-dec/ttusb_dec.c driver, aka CID-a10feaf8c464.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3689
722	CVE-2019-19532	MEDIUM	MEDIUM	In the Linux kernel before 5.3.9, there are multiple out-of-bounds write bugs that can be caused by a malicious USB device in the Linux kernel HID drivers, aka CID-d9d4b1e46d95. This affects drivers/hid/hid-axff.c, drivers/hid/hid-dr.c, drivers/hid/hid-emsff.c, drivers/hid/hid-gaff.c, drivers/hid/hid-holtekff.c, drivers/hid/hid-lg2ff.c, drivers/hid/hid-lg3ff.c, drivers/hid/hid-lg4ff.c, drivers/hid/hid-lgff.c, drivers/hid/hid-logitech-hidpp.c, drivers/hid/hid-microsoft.c, drivers/hid/hid-sony.c, drivers/hid/hid-tmff.c, and drivers/hid/hid-zpff.c.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	10.20.3.0	LIN1019-3690
723	CVE-2019-19531	MEDIUM	MEDIUM	In the Linux kernel before 5.2.9, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/usb/misc/yurex.c driver, aka CID-fc05481b2fca.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3691
724	CVE-2019-19530	MEDIUM	MEDIUM	In the Linux kernel before 5.2.10, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/usb/class/cdc-acm.c driver, aka CID-c52873e5a1ef.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3692
725	CVE-2019-19529	MEDIUM	MEDIUM	In the Linux kernel before 5.3.11, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/net/can/usb/mcba_usb.c driver, aka CID-4d6636498c41.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3693
726	CVE-2019-19528	MEDIUM	MEDIUM	In the Linux kernel before 5.3.7, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/usb/misc/iowarrior.c driver, aka CID-edc4746f253d.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3694
727	CVE-2019-19527	MEDIUM	MEDIUM	In the Linux kernel before 5.2.10, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/hid/usbhid/hiddev.c driver, aka CID-9c09b214f30e.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3695
728	CVE-2019-19526	MEDIUM	MEDIUM	In the Linux kernel before 5.3.9, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/nfc/pn533/usb.c driver, aka CID-6af3aa57a098.	linux	Unchanged	Not vulnerable	Investigate	10.17.41.19	10.18.44.14	10.19.45.3	10.20.3.0	LIN1019-3696
729	CVE-2019-19525	MEDIUM	MEDIUM	In the Linux kernel before 5.3.6, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/net/ieee802154/atusb.c driver, aka CID-7fd25e6fc035.	linux	Unchanged	Not vulnerable	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.6	Not vulnerable	LIN1019-3697
730	CVE-2019-19524	MEDIUM	MEDIUM	In the Linux kernel before 5.3.12, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/input/ff-memless.c driver, aka CID-fa3a5a1880c9.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	10.20.3.0	LIN1019-3698
731	CVE-2019-19523	MEDIUM	MEDIUM	In the Linux kernel before 5.3.7, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/usb/misc/adutux.c driver, aka CID-44efc269db79.	linux	Unchanged	Investigate	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3699
732	CVE-2019-19481	MEDIUM	HIGH	An issue was discovered in OpenSC through 0.19.0 and 0.20.x through 0.20.0-rc3. libopensc/card-cac1.c mishandles buffer limits for CAC certificates.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3752
733	CVE-2019-19480	MEDIUM	HIGH	An issue was discovered in OpenSC through 0.19.0 and 0.20.x through 0.20.0-rc3. libopensc/pkcs15-prkey.c has an incorrect free operation in sc_pkcs15_decode_prkdf_entry.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3751
734	CVE-2019-19479	LOW	MEDIUM	An issue was discovered in OpenSC through 0.19.0 and 0.20.x through 0.20.0-rc3. libopensc/card-setcos.c has an incorrect read operation during parsing of a SETCOS file attribute.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3750
735	CVE-2019-19462	MEDIUM	MEDIUM	relay_open in kernel/relay.c in the Linux kernel through 5.4.1 allows local users to cause a denial of service (such as relay blockage) by triggering a NULL alloc_percpu result.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1019-3700
736	CVE-2019-19449	MEDIUM	HIGH	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can lead to slab-out-of-bounds read access in f2fs_build_segment_manager in fs/f2fs/segment.c, related to init_min_max_mtime in fs/f2fs/segment.c (because the second argument to get_seg_entry is not validated).	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1019-3720
737	CVE-2019-19448	MEDIUM	HIGH	In the Linux kernel 5.0.21 and 5.3.11, mounting a crafted btrfs filesystem image, performing some operations, and then making a syncfs system call can lead to a use-after-free in try_merge_free_space in fs/btrfs/free-space-cache.c because the pointer to a left data structure can be the same as the pointer to a right data structure.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1019-3721
738	CVE-2019-19447	MEDIUM	HIGH	In the Linux kernel 5.0.21, mounting a crafted ext4 filesystem image, performing some operations, and unmounting can lead to a use-after-free in ext4_put_super in fs/ext4/super.c, related to dump_orphan_list in fs/ext4/super.c.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1019-3722
739	CVE-2019-19391	MEDIUM	CRITICAL	** DISPUTED ** In LuaJIT through 2.0.5, as used in Moonjit before 2.1.2 and other products, debug.getinfo has a type confusion issue that leads to arbitrary memory write or read operations, because certain cases involving valid stack levels and > options are mishandled. NOTE: The LuaJIT project owner states that the debug libary is unsafe by definition and that this is not a vulnerability. When LuaJIT was originally developed, the expectation was that the entire debug library had no security guarantees and thus it made no sense to assign CVEs. However, not all users of later LuaJIT derivatives share this perspective.	luajit	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3754
740	CVE-2019-19378	MEDIUM	HIGH	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image can lead to slab-out-of-bounds write access in index_rbio_pages in fs/btrfs/raid56.c.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1019-3701
741	CVE-2019-19377	MEDIUM	HIGH	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image, performing some operations, and unmounting can lead to a use-after-free in btrfs_queue_work in fs/btrfs/async-thread.c.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1019-3702
742	CVE-2019-19344	MEDIUM	MEDIUM	There is a use-after-free issue in all samba 4.9.x versions before 4.9.18, all samba 4.10.x versions before 4.10.12 and all samba 4.11.x versions before 4.11.5, essentially due to a call to realloc() while other local variables still point at the original buffer.	samba	Unchanged	Not vulnerable	Not vulnerable	10.17.41.20	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3964

	A	B	C	D	E	F	G	H	I	J	K	L	M
743	CVE-2019-19337	MEDIUM	MEDIUM	A flaw was found in Red Hat Ceph Storage version 3 in the way the Ceph RADOS Gateway daemon handles S3 requests. An authenticated attacker can abuse this flaw by causing a remote denial of service by sending a specially crafted HTTP Content-Length header to the Ceph RADOS Gateway server.	ceph	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3846
744	CVE-2019-19332	MEDIUM	MEDIUM	An out-of-bounds memory write issue was found in the Linux Kernel, version 3.13 through 5.4, in the way the Linux kernel's KVM hypervisor handled the 'KVM_GET_EMULATED_CPUID' ioctl(2) request to get CPUID features emulated by the KVM hypervisor. A user or process able to access the '/dev/kvm' device could use this flaw to crash the system, resulting in a denial of service.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.4	10.20.6.0	LIN1019-3920
745	CVE-2019-19319	MEDIUM	HIGH	In the Linux kernel 5.0.21, a setxattr operation, after a mount of a crafted ext4 image, can cause a slab-out-of-bounds write access because of an ext4_xattr_set_entry use-after-free in fs/ext4/xattr.c when a large old_size value is used in a memset call.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1019-3648
746	CVE-2019-19318	MEDIUM	MEDIUM	In the Linux kernel 5.3.11, mounting a crafted btrfs image twice can cause an rwsem_down_write_slowpath use-after-free because (in rwsem_can_spin_on_owner in kernel/locking/rwsem.c) rwsem_owner_flags returns an already freed pointer.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3649
747	CVE-2019-19317	HIGH	CRITICAL	lookupName in resolve.c in SQLite 3.30.1 omits bits from the colUsed bitmask in the case of a generated column, which allows attackers to cause a denial of service or possibly have unspecified other impact.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3718
748	CVE-2019-19272	MEDIUM	HIGH	An issue was discovered in tls_verify_crl in ProFTPD before 1.3.6. Direct dereference of a NULL pointer (a variable initialized to NULL) leads to a crash when validating the certificate of a client connecting to the server in a TLS client/server mutual-authentication setup.	proftpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3598
749	CVE-2019-19271	MEDIUM	HIGH	An issue was discovered in tls_verify_crl in ProFTPD before 1.3.6. A wrong iteration variable, used when checking a client certificate against CRL entries (installed by a system administrator), can cause some CRL entries to be ignored, and can allow clients whose certificates have been revoked to proceed with a connection to the server.	proftpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3599
750	CVE-2019-19270	MEDIUM	HIGH	An issue was discovered in tls_verify_crl in ProFTPD through 1.3.6b. Failure to check for the appropriate field of a CRL entry (checking twice for subject, rather than once for subject and once for issuer) prevents some valid CRLs from being taken into account, and can allow clients whose certificates have been revoked to proceed with a connection to the server.	proftpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3600
751	CVE-2019-19269	MEDIUM	MEDIUM	An issue was discovered in tls_verify_crl in ProFTPD through 1.3.6b. A dereference of a NULL pointer may occur. This pointer is returned by the OpenSSL sk_X509_REVOKED_value() function when encountering an empty CRL installed by a system administrator. The dereference occurs when validating the certificate of a client connecting to the server in a TLS client/server mutual-authentication setup.	proftpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3707
752	CVE-2019-19252	MEDIUM	HIGH	vcs_write in drivers/tty/vt/vc_screen.c in the Linux kernel through 5.3.13 does not prevent write access to vcsu devices, aka CID-0c9acb1af77a.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	Not vulnerable	LIN1019-3596
753	CVE-2019-19244	MEDIUM	HIGH	sqlite3Select in select.c in SQLite 3.30.1 allows a crash if a sub-select uses both DISTINCT and window functions, and also has certain ORDER BY usage.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.6.0	LIN1019-3602
754	CVE-2019-19242	MEDIUM	HIGH	SQLite 3.30.1 mishandles pExpr->y.pTab, as demonstrated by the TK_COLUMN case in sqlite3ExprCodeTarget in expr.c.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	Not vulnerable	LIN1019-3660
755	CVE-2019-19241	MEDIUM	HIGH	In the Linux kernel before 5.4.2, the io_uring feature leads to requests that inadvertently have UID 0 and full capabilities, aka CID-181e448d8709. This is related to fs/io-wq.c, fs/io_uring.c, and net/socket.c. For example, an attacker can bypass intended restrictions on adding an IPv4 address to the loopback interface. This occurs because IORING_OP_SENDMSG operations, although requested in the context of an unprivileged user, are sometimes performed by a kernel worker thread without considering that context.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.3	Not vulnerable	LIN1019-3801
756	CVE-2019-19234	MEDIUM	HIGH	In Sudo through 1.8.29, the fact that a user has been blocked (e.g., by using the ! character in the shadow file instead of a password hash) is not considered, allowing an attacker (who has access to a Runas ALL sudoer account) to impersonate any blocked user.	shadow	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3816
757	CVE-2019-19232	MEDIUM	HIGH	In Sudo through 1.8.29, an attacker with access to a Runas ALL sudoer account can impersonate a nonexistent user by invoking sudo with a numeric uid that is not associated with any user.	sudo	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3817
758	CVE-2019-19227	LOW	MEDIUM	In the AppleTalk subsystem in the Linux kernel before 5.1, there is a potential NULL pointer dereference because register_snap_client may return NULL. This will lead to denial of service in net/appletalk/aarp.c and net/appletalk/ddp.c, as demonstrated by unregister_snap_client, aka CID-9804501fa122.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	Not vulnerable	Not vulnerable	LIN1019-3582
759	CVE-2019-19221	LOW	MEDIUM	In Libarchive 3.4.0, archive_wstring_append_from_mbs in archive_string.c has an out-of-bounds read because of an incorrect mbrtowc or mbtowc call. For example, bsdtar crashes via a crafted archive.	libarchive	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3578

	A	B	C	D	E	F	G	H	I	J	K	L	M
760	CVE-2019-19126	LOW	LOW	On the x86-64 architecture, the GNU C Library (aka glibc) before 2.31 fails to ignore the LD_PREFER_MAP_32BIT_EXEC environment variable during program execution after a security transition, allowing local attackers to restrict the possible mapping addresses for loaded libraries and thus bypass ASLR for a setuid program.	glibc	Unchanged	Not vulnerable	Vulnerable	10.17.41.20	10.18.44.15	10.19.45.6	10.20.3.0	LIN1019-3566
761	CVE-2019-19083	HIGH	HIGH	Memory leaks in *clock_source_create() functions under drivers/gpu/drm/amd/display/dc in the Linux kernel before 5.3.8 allow attackers to cause a denial of service (memory consumption). This affects the dce112_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce112/dce112_resource.c, the dce100_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce100/dce100_resource.c, the dcn10_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dcn10/dcn10_resource.c, the dcn20_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dcn20/dcn20_resource.c, the dce120_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce120/dce120_resource.c, the dce110_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce110/dce110_resource.c, and the dce80_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce80/dce80_resource.c, aka CID-055e547478a1.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3478
762	CVE-2019-19082	HIGH	HIGH	Memory leaks in *create_resource_pool() functions under drivers/gpu/drm/amd/display/dc in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption). This affects the dce120_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dce120/dce120_resource.c, the dce110_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dce110/dce110_resource.c, the dce100_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dce100/dce100_resource.c, the dcn10_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dcn10/dcn10_resource.c, and the dce112_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dce112/dce112_resource.c, aka CID-104c307147ad.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3479
763	CVE-2019-19081	HIGH	HIGH	A memory leak in the nfp_flower_spawn_vnic_reprs() function in drivers/net/ethernet/netronome/nfp/flower/main.c in the Linux kernel before 5.3.4 allows attackers to cause a denial of service (memory consumption), aka CID-8ce39eb5a67a.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.13	10.19.45.1	10.20.3.0	LIN1019-3480
764	CVE-2019-19080	HIGH	HIGH	Four memory leaks in the nfp_flower_spawn_phy_reprs() function in drivers/net/ethernet/netronome/nfp/flower/main.c in the Linux kernel before 5.3.4 allow attackers to cause a denial of service (memory consumption), aka CID-8572cea1461a.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.13	10.19.45.1	10.20.3.0	LIN1019-3481
765	CVE-2019-19079	HIGH	HIGH	A memory leak in the qrtr_tun_write_iter() function in net/qrtr/tun.c in the Linux kernel before 5.3 allows attackers to cause a denial of service (memory consumption), aka CID-a21b7f0cff19.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3482
766	CVE-2019-19078	HIGH	HIGH	A memory leak in the ath10k_usb_hif_tx_sg() function in drivers/net/wireless/ath/ath10k/usb.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-b8d17e7d93d2.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3483
767	CVE-2019-19077	HIGH	HIGH	A memory leak in the bnxt_re_create_srq() function in drivers/infiniband/hw/bnxt_re/ib_verbs.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering copy to udata failures, aka CID-4a9d46a9fe14.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3484
768	CVE-2019-19076	HIGH	HIGH	A memory leak in the nfp_abm_u32_knode_replace() function in drivers/net/ethernet/netronome/nfp/abm/cls.c in the Linux kernel before 5.3.6 allows attackers to cause a denial of service (memory consumption), aka CID-78beef629fd9.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.3.0	LIN1019-3485
769	CVE-2019-19075	HIGH	HIGH	A memory leak in the ca8210_probe() function in drivers/net/ieee802154/ca8210.c in the Linux kernel before 5.3.8 allows attackers to cause a denial of service (memory consumption) by triggering ca8210_get_platform_data() failures, aka CID-6402939ec86e.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3486
770	CVE-2019-19074	HIGH	HIGH	A memory leak in the ath9k_wmi_cmd() function in drivers/net/wireless/ath/ath9k/wmi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-728c1e2a05e4.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3488
771	CVE-2019-19073	HIGH	HIGH	Memory leaks in drivers/net/wireless/ath/ath9k/htc_hst.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering wait_for_completion_timeout() failures. This affects the htc_config_pipe_credits() function, the htc_setup_complete() function, and the htc_connect_service() function, aka CID-853acf7caf10.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3489

	A	B	C	D	E	F	G	H	I	J	K	L	M
772	CVE-2019-19072	HIGH	HIGH	A memory leak in the predicate_parse() function in kernel/trace/trace_events_filter.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-96c5c6e6a5b6.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3490
773	CVE-2019-19071	HIGH	HIGH	A memory leak in the rsi_send_beacon() function in drivers/net/wireless/rsi/rsi_91x_mgmt.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering rsi_prepare_beacon() failures, aka CID-d563131ef23c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.2	10.20.3.0	LIN1019-3491
774	CVE-2019-19070	HIGH	HIGH	** DISPUTED ** A memory leak in the spi_gpio_probe() function in drivers/spi/spi-gpio.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering devm_add_action_or_reset() failures, aka CID-d3b0ffa1d75d. NOTE: third parties dispute the relevance of this because the system must have already been out of memory before the probe began.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.12.0	LIN1019-3492
775	CVE-2019-19069	HIGH	HIGH	A memory leak in the fastrpc_dma_buf_attach() function in drivers/misc/fastrpc.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering dma_get_sgtable() failures, aka CID-fc739a058d99.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.3.0	LIN1019-3493
776	CVE-2019-19068	HIGH	HIGH	A memory leak in the rtl8xxxu_submit_int_urb() function in drivers/net/wireless/realtek/rtl8xxxu/rtl8xxxu_core.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-a2cdd07488e6.	linux	Unchanged	Not vulnerable	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3494
777	CVE-2019-19067	HIGH	HIGH	** DISPUTED ** Four memory leaks in the acp_hw_init() function in drivers/gpu/drm/amd/amdgpu/amdgpu_acp.c in the Linux kernel before 5.3.8 allow attackers to cause a denial of service (memory consumption) by triggering mfd_add_hotplug_devices() or pm_genpd_add_device() failures, aka CID-57be09c6e874. NOTE: third parties dispute the relevance of this because the attacker must already have privileges for module loading.	linux	Unchanged	Not vulnerable	Vulnerable	Vulnerable	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3495
778	CVE-2019-19066	HIGH	HIGH	A memory leak in the bfad_im_get_stats() function in drivers/scsi/bfa/bfad_attr.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering bfa_port_get_stats() failures, aka CID-0e62395da2bd.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3496
779	CVE-2019-19065	HIGH	HIGH	A memory leak in the sdma_init() function in drivers/infiniband/hw/hfi1/sdma.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering rhashtable_init() failures, aka CID-34b3be18a04e.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3498
780	CVE-2019-19064	HIGH	HIGH	** DISPUTED ** A memory leak in the fsl_lpspi_probe() function in drivers/spi/spi-fsl-lpspi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering pm_runtime_get_sync() failures, aka CID-057b8945f78f. NOTE: third parties dispute the relevance of this because an attacker cannot realistically control these failures at probe time.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.3.0	LIN1019-3500
781	CVE-2019-19063	HIGH	HIGH	Two memory leaks in the rtl_usb_probe() function in drivers/net/wireless/realtek/rtlwifi/usb.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption), aka CID-3f9361695113.	linux	Unchanged	Not vulnerable	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3501
782	CVE-2019-19062	HIGH	HIGH	A memory leak in the crypto_report() function in crypto/crypto_user_base.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering crypto_report_alg() failures, aka CID-ffdde5932042.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	Not vulnerable	LIN1019-3502
783	CVE-2019-19061	HIGH	HIGH	A memory leak in the adis_update_scan_mode_burst() function in drivers/iio/imu/adis_buffer.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-9c0530e898f3.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3504
784	CVE-2019-19060	HIGH	HIGH	A memory leak in the adis_update_scan_mode() function in drivers/iio/imu/adis_buffer.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-ab612b1daf41.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3505
785	CVE-2019-19059	HIGH	HIGH	Multiple memory leaks in the iwl_pcie_ctxt_info_gen3_init() function in drivers/net/wireless/intel/iwlwifi/pcie/ctxt-info-gen3.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering iwl_pcie_init_fw_sec() or dma_alloc_coherent() failures, aka CID-0f4f199443fa.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.3.0	LIN1019-3507
786	CVE-2019-19058	HIGH	HIGH	A memory leak in the alloc_sgtable() function in drivers/net/wireless/intel/iwlwifi/fw/dbg.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering alloc_page() failures, aka CID-b4b814fec1a5.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3509
787	CVE-2019-19057	HIGH	HIGH	Two memory leaks in the mwifiex_pcie_init_evt_ring() function in drivers/net/wireless/marvell/mwifiex/pcie.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering mwifiex_map_pci_memory() failures, aka CID-d10dcb615c8e.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3511
788	CVE-2019-19056	HIGH	HIGH	A memory leak in the mwifiex_pcie_alloc_cmdrsp_buf() function in drivers/net/wireless/marvell/mwifiex/pcie.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering mwifiex_map_pci_memory() failures, aka CID-db8fd2cde932.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	10.20.3.0	LIN1019-3512

	A	B	C	D	E	F	G	H	I	J	K	L	M
789	CVE-2019-19055	HIGH	HIGH	** DISPUTED ** A memory leak in the nl80211_get_ftm_responder_stats() function in net/wireless/nl80211.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering nl80211hdr_put() failures, aka CID-1399c59fa929. NOTE: third parties dispute the relevance of this because it occurs on a code path where a successful allocation has already occurred.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.3.0	LIN1019-3514
790	CVE-2019-19054	HIGH	HIGH	A memory leak in the cx23888_ir_probe() function in drivers/media/pci/cx23885/cx23888-ir.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering kfifo_alloc() failures, aka CID-a7b2df76b42b.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3515
791	CVE-2019-19053	HIGH	HIGH	A memory leak in the rpmsg_eptdev_write_iter() function in drivers/rpmsg/rpmsg_char.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering copy_from_iter_full() failures, aka CID-bbe692e349e2.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.5	10.20.6.0	LIN1019-3517
792	CVE-2019-19052	HIGH	HIGH	A memory leak in the gs_can_open() function in drivers/net/can/usb/gs_usb.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-fb5be6a7b486.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3518
793	CVE-2019-19051	HIGH	HIGH	A memory leak in the i2400m_op_rfkill_sw_toggle() function in drivers/net/wimax/i2400m/op-rfkill.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-6f3ef5c25cc7.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.13	10.19.45.2	10.20.3.0	LIN1019-3519
794	CVE-2019-19050	HIGH	HIGH	A memory leak in the crypto_reportstat() function in crypto/crypto_user_stat.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering crypto_reportstat_alg() failures, aka CID-c03b04dcdba1.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	Not vulnerable	LIN1019-3522
795	CVE-2019-19049	HIGH	HIGH	** DISPUTED ** A memory leak in the unittest_data_add() function in drivers/of/unittest.c in the Linux kernel before 5.3.10 allows attackers to cause a denial of service (memory consumption) by triggering of_fdt_unflatten_tree() failures, aka CID-e13de8fe0d6a. NOTE: third parties dispute the relevance of this because unittest.c can only be reached during boot.	linux	Unchanged	Vulnerable	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	10.20.3.0	LIN1019-3523
796	CVE-2019-19048	HIGH	HIGH	A memory leak in the crypto_reportstat() function in drivers/virt/vboxguest/vboxguest_utils.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering copy_form_user() failures, aka CID-e0b0cb938864.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.2	10.20.3.0	LIN1019-3524
797	CVE-2019-19047	HIGH	HIGH	A memory leak in the mlx5_fw_fatal_reporter_dump() function in drivers/net/ethernet/mellanox/mlx5/core/health.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering mlx5_crdump_collect() failures, aka CID-c7ed6d0183d5.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.20.3.0	LIN1019-3526
798	CVE-2019-19046	HIGH	HIGH	** DISPUTED ** A memory leak in the __ipmi_bmc_register() function in drivers/char/ipmi/ipmi_msghandler.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering ida_simple_get() failure, aka CID-4aa7afb0ee20. NOTE: third parties dispute the relevance of this because an attacker cannot realistically control this failure at probe time.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3527
799	CVE-2019-19045	HIGH	HIGH	A memory leak in the mlx5_fpga_conn_create_cq() function in drivers/net/ethernet/mellanox/mlx5/core/fpga/conn.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering mlx5_vector2eqn() failures, aka CID-c8c2a057fdc7.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.2	10.20.3.0	LIN1019-3528
800	CVE-2019-19044	HIGH	HIGH	Two memory leaks in the v3d_submit_cl_ioctl() function in drivers/gpu/drm/v3d/v3d_gem.c in the Linux kernel before 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering kcalloc() or v3d_job_init() failures, aka CID-29cd13cfd762.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.20.3.0	LIN1019-3530
801	CVE-2019-19043	HIGH	HIGH	A memory leak in the i40e_setup_macvlans() function in drivers/net/ethernet/intel/i40e/i40e_main.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering i40e_setup_channel() failures, aka CID-27d461333459.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3532
802	CVE-2019-19039	LOW	MEDIUM	__btrfs_free_extent in fs/btrfs/extent-tree.c in the Linux kernel through 5.3.12 calls btrfs_print_leaf in a certain ENOENT case, which allows local users to obtain potentially sensitive information about register values via the dmesg program.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1019-3570
803	CVE-2019-19037	MEDIUM	MEDIUM	ext4_empty_dir in fs/ext4/namei.c in the Linux kernel through 5.3.12 allows a NULL pointer dereference because ext4_read_dirblock(inode,0,DIRENT_HTREE) can be zero.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.6	Investigate	LIN1019-3571
804	CVE-2019-19036	MEDIUM	MEDIUM	btrfs_root_node in fs/btrfs/ctree.c in the Linux kernel through 5.3.12 allows a NULL pointer dereference because rcu_dereference(root->node) can be zero.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1019-3572
805	CVE-2019-19011	MEDIUM	HIGH	MiniUPnP ngiflib 0.4 has a NULL pointer dereference in GifIndexToTrueColor in ngiflib.c via a file that lacks a palette.	miniupnpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3477
806	CVE-2019-18885	LOW	MEDIUM	fs/btrfs/volumes.c in the Linux kernel before 5.1 allows a btrfs_verify_dev_extents NULL pointer dereference via a crafted btrfs image because fs_devices->devices is mishandled within find_device, aka CID-09ba3bc9dd15.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	Not vulnerable	Not vulnerable	LIN1019-3467

	A	B	C	D	E	F	G	H	I	J	K	L	M
807	CVE-2019-18874	MEDIUM	HIGH	psutil (aka python-psutil) through 5.6.5 can have a double free. This occurs because of refcount mishandling within a while or for loop that converts system data into a Python object.	python-psutil	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3436
808	CVE-2019-18860	MEDIUM	MEDIUM	Squid before 4.9, when certain web browsers are used, mishandles HTML in the host (aka hostname) parameter to cachemgr.cgi.	squid	Updated	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4158
809	CVE-2019-18853	MEDIUM	MEDIUM	ImageMagick before 7.0.9-0 allows remote attackers to cause a denial of service because XML_PARSE_HUGE is not properly restricted in coders/svg.c, related to SVG and libxml2.	imagemagick	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3437
810	CVE-2019-18840	MEDIUM	HIGH	In wolfSSL 4.1.0 through 4.2.0c, there are missing sanity checks of memory accesses in parsing ASN.1 certificate data while handshaking. Specifically, there is a one-byte heap-based buffer overflow inside the DecodedCert structure in GetName in wolfcrypt/src/asn.c because the domain name location index is mishandled. Because a pointer is overwritten, there is an invalid free.	wolfssl	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3438
811	CVE-2019-18814	HIGH	CRITICAL	An issue was discovered in the Linux kernel through 5.3.9. There is a use-after-free when aa_label_parse() fails in aa_audit_rule_init() in security/apparmor/audit.c.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3379
812	CVE-2019-18813	HIGH	HIGH	A memory leak in the dwc3_pci_probe() function in drivers/usb/dwc3/dwc3-pci.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering platform_device_add_properties() failures, aka CID-9bbfceea12a8.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.3.0	LIN1019-3380
813	CVE-2019-18812	HIGH	HIGH	A memory leak in the sof_dfsentry_write() function in sound/soc/sof/debug.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-c0a333d842ef.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.20.3.0	LIN1019-3381
814	CVE-2019-18811	HIGH	HIGH	A memory leak in the sof_set_get_large_ctrl_data() function in sound/soc/sof/ipc.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering sof_get_ctrl_copy_params() failures, aka CID-45c1380358b1.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.3.0	LIN1019-3382
815	CVE-2019-18810	HIGH	HIGH	A memory leak in the komeda_wb_connector_add() function in drivers/gpu/drm/arm/display/komeda/komeda_wb_connector.c in the Linux kernel before 5.3.8 allows attackers to cause a denial of service (memory consumption) by triggering drm_writeback_connector_init() failures, aka CID-a0ecd6fdbf5d.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.20.3.0	LIN1019-3383
816	CVE-2019-18809	HIGH	HIGH	A memory leak in the af9005_identify_state() function in drivers/media/usb/dvb-usb/af9005.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-2289adbfa559.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.14	10.19.45.2	10.20.3.0	LIN1019-3384
817	CVE-2019-18808	MEDIUM	HIGH	A memory leak in the ccp_run_sha_cmd() function in drivers/crypto/ccp/ccp-ops.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-128c66429247.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.14	10.19.45.2	10.20.3.0	LIN1019-3385
818	CVE-2019-18807	MEDIUM	HIGH	Two memory leaks in the sja1105_static_config_upload() function in drivers/net/dsa/sja1105/sja1105_spi.c in the Linux kernel before 5.3.5 allow attackers to cause a denial of service (memory consumption) by triggering static_config_buf_prepare_for_upload() or sja1105_inhibit_tx() failures, aka CID-68501df92d11.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.3.0	LIN1019-3386
819	CVE-2019-18806	LOW	MEDIUM	A memory leak in the ql_alloc_large_buffers() function in drivers/net/ethernet/qlogic/qla3xxx.c in the Linux kernel before 5.3.5 allows local users to cause a denial of service (memory consumption) by triggering pci_dma_mapping_error() failures, aka CID-1acb82a7a9f.	linux	Unchanged	8.0.0.32	9.0.0.24	10.17.41.19	10.18.44.13	Not vulnerable	Investigate	LIN1019-3387
820	CVE-2019-18805	HIGH	CRITICAL	An issue was discovered in net/ipv4/sysctl_net_ipv4.c in the Linux kernel before 5.0.11. There is a net/ipv4/tcp_input.c signed integer overflow in tcp_ack_update_rtt() when userspace writes a very large integer to /proc/sys/net/ipv4/tcp_min_rtt_wlen, leading to a denial of service or possibly unspecified other impact, aka CID-19fad20d15a6.	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.19	Not vulnerable	Not vulnerable	Investigate	LIN1019-3388
821	CVE-2019-18792	MEDIUM	CRITICAL	An issue was discovered in Suricata 5.0.0. It is possible to bypass/evade any tcp based signature by overlapping a TCP segment with a fake FIN packet. The fake FIN packet is injected just before the PUSH ACK packet we want to bypass. The PUSH ACK packet (containing the data) will be ignored by Suricata because it overlaps the FIN packet (the sequence and ack number are identical in the two packets). The client will ignore the fake FIN packet because the ACK flag is not set. Both linux and windows clients are ignoring the injected packet.	suricata	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3889
822	CVE-2019-18786	LOW	MEDIUM	In the Linux kernel through 5.3.8, f->fmt.sdr.reserved is uninitialized in rcar_drif_g_fmt_sdr_cap in drivers/media/platform/rcar_drif.c, which could cause a memory disclosure problem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.2	10.20.3.0	LIN1019-3291
823	CVE-2019-18684	MEDIUM	HIGH	** DISPUTED ** Sudo through 1.8.29 allows local users to escalate to root if they have write access to file descriptor 3 of the sudo process. This occurs because of a race condition between determining a uid, and the setresuid and openat system calls. The attacker can write ALL ALL=(ALL) NOPASSWD:ALL to /proc/#####/fd/3 at a time when Sudo is prompting for a password. NOTE: This has been disputed due to the way Linux /proc works. It has been argued that writing to /proc/#####/fd/3 would only be viable if you had permission to write to /etc/sudoers. Even with write permission to /proc/#####/fd/3, it would not help you write to /etc/sudoers.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3292

	A	B	C	D	E	F	G	H	I	J	K	L	M
824	CVE-2019-18683	MEDIUM	HIGH	An issue was discovered in drivers/media/platform/vivid in the Linux kernel through 5.3.8. It is exploitable for privilege escalation on some Linux distributions where local users have /dev/video0 access, but only if the driver happens to be loaded. There are multiple race conditions during streaming stopping in this driver (part of the V4L2 subsystem). These issues are caused by wrong mutex locking in vivid_stop_generating_vid_cap(), vivid_stop_generating_vid_out(), sdr_cap_stop_streaming(), and the corresponding kthreads. At least one of these race conditions leads to a use-after-free.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3293
825	CVE-2019-18680	HIGH	HIGH	An issue was discovered in the Linux kernel 4.4.x before 4.4.195. There is a NULL pointer dereference in rds_tcp_kill_sock() in net/rds/tcp.c that will cause denial of service, aka CID-9157ae4aed0.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1019-3294
826	CVE-2019-18679	MEDIUM	HIGH	An issue was discovered in Squid 2.x, 3.x, and 4.x through 4.8. Due to incorrect data management, it is vulnerable to information disclosure when processing HTTP Digest Authentication. Nonce tokens contain the raw byte value of a pointer that sits within heap memory allocation. This information reduces ASLR protections and may aid attackers isolating memory areas to target for remote code execution attacks.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3651
827	CVE-2019-18678	MEDIUM	MEDIUM	An issue was discovered in Squid 3.x and 4.x through 4.8. It allows attackers to smuggle HTTP requests through frontend software to a Squid instance that splits the HTTP Request pipeline differently. The resulting Response messages corrupt caches (between a client and Squid) with attacker-controlled content at arbitrary URLs. Effects are isolated to software between the attacker client and Squid. There are no effects on Squid itself, nor on any upstream servers. The issue is related to a request header containing whitespace between a header name and a colon.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3652
828	CVE-2019-18677	MEDIUM	MEDIUM	An issue was discovered in Squid 3.x and 4.x through 4.8 when the append_domain setting is used (because the appended characters do not properly interact with hostname length restrictions). Due to incorrect message processing, it can inappropriately redirect traffic to origins it should not be delivered to.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3653
829	CVE-2019-18676	MEDIUM	HIGH	An issue was discovered in Squid 3.x and 4.x through 4.8. Due to incorrect input validation, there is a heap-based buffer overflow that can result in Denial of Service to all clients using the proxy. Severity is high due to this vulnerability occurring before normal security checks; any remote client that can reach the proxy port can trivially perform the attack via a crafted URI scheme.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3654
830	CVE-2019-18675	HIGH	HIGH	The Linux kernel through 5.3.13 has a start_offset+size Integer Overflow in cpia2_remap_buffer in drivers/media/usb/cpia2/cpia2_core.c because cpia2 has its own mmap implementation. This allows local users (with /dev/video0 access) to obtain read and write permissions on kernel physical pages, which can possibly result in a privilege escalation.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1019-3601
831	CVE-2019-18660	LOW	MEDIUM	The Linux kernel through 5.3.13 on powerpc allows Information Exposure because the Spectre-RSB mitigation is not in place for all applicable CPUs, aka CID-39e72bf96f58. This is related to arch/powerpc/kernel/entry_64.S and arch/powerpc/kernel/security.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3650
832	CVE-2019-18634	MEDIUM	HIGH	In Sudo before 1.8.26, if pwfeedback is enabled in /etc/sudoers, users can trigger a stack-based buffer overflow in the privileged sudo process. (pwfeedback is a default setting in Linux Mint and elementary OS; however, it is NOT the default for upstream and many other packages, and would exist only if enabled by an administrator.) The attacker needs to deliver a long string to the stdin of getln() in tgetpass.c.	sudo	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.5	Not vulnerable	LIN1019-3986
833	CVE-2019-18625	MEDIUM	HIGH	An issue was discovered in Suricata 5.0.0. It was possible to bypass/evade any tcp based signature by faking a closed TCP session using an evil server. After the TCP SYN packet, it is possible to inject a RST ACK and a FIN ACK packet with a bad TCP Timestamp option. The client will ignore the RST ACK and the FIN ACK packets because of the bad TCP Timestamp option. Both linux and windows client are ignoring the injected packets.	suricata	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3890
834	CVE-2019-18622	HIGH	CRITICAL	An issue was discovered in phpMyAdmin before 4.9.2. A crafted database/table name can be used to trigger a SQL injection attack through the designer feature.	phpmyadmin	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	10.20.3.0	LIN1019-3581
835	CVE-2019-18609	HIGH	CRITICAL	An issue was discovered in amqp_handle_input in amqp_connection.c in rabbitmq-c 0.9.0. There is an integer overflow that leads to heap memory corruption in the handling of CONNECTION_STATE_HEADER. A rogue server could return a malicious frame header that leads to a smaller target_size value than needed. This condition is then carried on to a memcpy function that copies too much data into a heap buffer.	rabbitmq-c	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.3	Not vulnerable	LIN1019-3782
836	CVE-2019-18408	MEDIUM	HIGH	archive_read_format_rar_read_data in archive_read_support_format_rar.c in libarchive before 3.4.0 has a use-after-free in a certain ARCHIVE_FAILED situation, related to Ppmd7_DecodeSymbol.	libarchive	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Investigate	LIN1018-5163

	A	B	C	D	E	F	G	H	I	J	K	L	M
837	CVE-2019-18397	MEDIUM	HIGH	A buffer overflow in the fribidi_get_par_embedding_levels_ex() function in lib/fribidi-bidi.c of GNU FriBidi through 1.0.7 allows an attacker to cause a denial of service or possibly execute arbitrary code by delivering crafted text content to a user, when this content is then rendered by an application that uses FriBidi for text layout calculations. Examples include any GNOME or GTK+ based application that uses Pango for text layout, as this internally uses FriBidi for bidirectional text layout. For example, the attacker can construct a crafted text file to be opened in GEdit, or a crafted IRC message to be viewed in HexChat.	fribidi	Unchanged	Won't Fix	Won't Fix	Won't Fix	10.18.44.13	10.19.45.2	Investigate	LIN1019-3450
838	CVE-2019-18391	LOW	MEDIUM	A heap-based buffer overflow in the vrend_renderer_transfer_write_iov function in vrend_renderer.c in virglrenderer through 0.8.0 allows guest OS users to cause a denial of service via VIRGL_CCMD_RESOURCE_INLINE_WRITE commands.	virglrenderer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.3	Not vulnerable	LIN1019-3842
839	CVE-2019-18390	LOW	HIGH	An out-of-bounds read in the vrend_blit_need_swizzle function in vrend_renderer.c in virglrenderer through 0.8.0 allows guest OS users to cause a denial of service via VIRGL_CCMD_BLIT commands.	virglrenderer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.3	Not vulnerable	LIN1019-3843
840	CVE-2019-18389	MEDIUM	HIGH	A heap-based buffer overflow in the vrend_renderer_transfer_write_iov function in vrend_renderer.c in virglrenderer through 0.8.0 allows guest OS users to cause a denial of service, or QEMU guest-to-host escape and code execution, via VIRGL_CCMD_RESOURCE_INLINE_WRITE commands.	virglrenderer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.3	Not vulnerable	LIN1019-3844
841	CVE-2019-18388	LOW	MEDIUM	A NULL pointer dereference in vrend_renderer.c in virglrenderer through 0.8.0 allows guest OS users to cause a denial of service via malformed commands.	virglrenderer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.3	Not vulnerable	LIN1019-3845
842	CVE-2019-18348	MEDIUM	MEDIUM	An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib in Python 3.x through 3.8.0. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the host component of a URL) followed by an HTTP header. This is similar to the CVE-2019-9740 query string issue and the CVE-2019-9947 path string issue. (This is not exploitable when glibc has CVE-2016-10739 fixed.)	python	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Not vulnerable	LIN1018-5159
843	CVE-2019-18282	MEDIUM	MEDIUM	The flow_dissector feature in the Linux kernel 4.3 through 5.x before 5.3.10 has a device tracking vulnerability, aka CID-5567441c84f. This occurs because the auto flowlabel of a UDP IPv6 packet relies on a 32-bit hashmd value as a secret, and because jhash (instead of siphash) is used. The hashmd value remains the same starting from boot time, and can be inferred by an attacker. This affects net/core/flow_dissector.c and related code.	linux	Unchanged	Not vulnerable	9.0.0.25	Investigate	10.18.44.15	10.19.45.3	10.20.6.0	LIN1019-3954
844	CVE-2019-18276	HIGH	CRITICAL	An issue was discovered in disable_priv_mode in shell.c in GNU Bash through 5.0 patch 11. By default, if Bash is run with its effective UID not equal to its real UID, it will drop privileges by setting its effective UID to its real UID. However, it does so incorrectly. On Linux and other systems that support saved UID functionality, the saved UID is not dropped. An attacker with command execution in the shell can use enable -f for runtime loading of a new builtin, which can be a shared object that calls setuid() and therefore regains privileges. However, binaries running with an effective UID of 0 are unaffected.	bash	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	10.20.3.0	LIN1019-3706
845	CVE-2019-18224	HIGH	CRITICAL	idn2_to_ascii_4i in lib/lookup.c in GNU libidn2 before 2.1.1 has a heap-based buffer overflow via a long domain string.	libidn2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.12	Not vulnerable	Investigate	LIN1018-5151
846	CVE-2019-18218	HIGH	CRITICAL	cdf_read_property_info in cdf.c in file through 5.37 does not restrict the number of CDF_VECTOR elements, which allows a heap-based buffer overflow (4-byte out-of-bounds write).	file	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.1	Not vulnerable	LIN1018-5152
847	CVE-2019-18217	MEDIUM	HIGH	ProFTPD before 1.3.6b and 1.3.7rc before 1.3.7rc2 allows remote unauthenticated denial-of-service due to incorrect handling of overly long commands because main.c in a child process enters an infinite loop.	proftpd	Unchanged	8.0.0.31	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5165
848	CVE-2019-18198	HIGH	HIGH	In the Linux kernel before 5.3.4, a reference count usage error in the fib6_rule_suppress() function in the fib6 suppression feature of net/ipv6/fib6_rules.c, when handling the FIB_LOOKUP_NOREF flag, can be exploited by a local attacker to corrupt memory, aka CID-ca7a03c41753.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Investigate	LIN1018-5112
849	CVE-2019-18197	MEDIUM	CRITICAL	In xsltCopyText in transform.c in libxslt 1.1.33, a pointer variable isn't reset under certain circumstances. If the relevant memory area happened to be freed and reused in a certain way, a bounds check could fail and memory outside a buffer could be written to, or uninitialized data could be disclosed.	libxslt	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.1	Not vulnerable	LIN1018-5111
850	CVE-2019-1798	Medium	MEDIUM	A vulnerability in the Portable Executable (PE) file scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a lack of proper input and validation checking mechanisms for PE files sent an affected device. An attacker could exploit this vulnerability by sending malformed PE files to the device running an affected version ClamAV Software. An exploit could allow the attacker to cause an out-of-bounds read condition, resulting in a crash that could result in a denial of service condition on an affected device.	clamav	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3875
851	CVE-2019-1789	MEDIUM	HIGH	ClamAV versions prior to 0.101.2 are susceptible to a denial of service (DoS) vulnerability. An out-of-bounds heap read condition may occur when scanning PE files. An example is Windows EXE and DLL files that have been packed using Aspack as a result of inadequate bound-checking.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	LIN1019-3300

	A	B	C	D	E	F	G	H	I	J	K	L	M
852	CVE-2019-1788	Medium	MEDIUM	A vulnerability in the Object Linking & Embedding (OLE2) file scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a lack of proper input and validation checking mechanisms for OLE2 files sent an affected device. An attacker could exploit this vulnerability by sending malformed OLE2 files to the device running an affected version ClamAV Software. An exploit could allow the attacker to cause an out-of-bounds write condition, resulting in a crash that could result in a denial of service condition on an affected device.	clamav	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3876
853	CVE-2019-1787	Medium	MEDIUM	A vulnerability in the Portable Document Format (PDF) scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a lack of proper data handling mechanisms within the device buffer while indexing remaining file data on an affected device. An attacker could exploit this vulnerability by sending crafted PDF files to an affected device. A successful exploit could allow the attacker to cause a heap buffer out-of-bounds read condition, resulting in a crash that could result in a denial of service condition on an affected device.	clamav	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3877
854	CVE-2019-1786	Medium	MEDIUM	A vulnerability in the Portable Document Format (PDF) scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and 0.101.0 could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a lack of proper data handling mechanisms within the device buffer while indexing remaining file data on an affected device. An attacker could exploit this vulnerability by sending crafted PDF files to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read condition, resulting in a crash that could result in a denial of service condition on an affected device.	clamav	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3878
855	CVE-2019-1785	Medium	HIGH	A vulnerability in the RAR file scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and 0.101.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a lack of proper error-handling mechanisms when processing nested RAR files sent to an affected device. An attacker could exploit this vulnerability by sending a crafted RAR file to an affected device. An exploit could allow the attacker to view or create arbitrary files on the targeted system.	clamav	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3879
856	CVE-2019-17666	HIGH	HIGH	rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel through 5.3.6 lacks a certain upper-bound check, leading to a buffer overflow.	linux	Unchanged	8.0.0.32	9.0.0.24	10.17.41.19	10.18.44.13	10.19.45.1	10.20.3.0	LIN1018-5113
857	CVE-2019-17596	MEDIUM	HIGH	Go before 1.12.11 and 1.3.x before 1.13.2 can panic upon an attempt to process network traffic containing an invalid DSA public key. There are several attack scenarios, such as traffic from a client to a server that verifies client certificates.	go	Unchanged	Not vulnerable	Won't Fix	10.17.41.19	10.18.44.12	10.19.45.1	Not vulnerable	LIN1018-5164
858	CVE-2019-17595	MEDIUM	MEDIUM	There is a heap-based buffer over-read in the fmt_entry function in tinfo/comp_hash.c in the terminfo library in ncurses before 6.1-20191012.	ncurses	Unchanged	8.0.0.31	9.0.0.24	10.17.41.20	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5098
859	CVE-2019-17594	MEDIUM	HIGH	There is a heap-based buffer over-read in the _nc_find_entry function in tinfo/comp_hash.c in the terminfo library in ncurses before 6.1-20191012.	ncurses	Unchanged	8.0.0.31	9.0.0.24	10.17.41.20	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5099
860	CVE-2019-17571	HIGH	CRITICAL	Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.	log4j1.2	Unchanged	8.0.0.33	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-12023
861	CVE-2019-17547	MEDIUM	HIGH	In ImageMagick before 7.0.8-62, TraceBezier in MagickCore/draw.c has a use-after-free.	imagemagick	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5093
862	CVE-2019-17546	MEDIUM	HIGH	tif_getimage.c in LibTIFF through 4.0.10, as used in GDAL through 3.0.1 and other products, has an integer overflow that potentially causes a heap-based buffer overflow via a crafted RGBA image, related to a Negative-size-param condition.	libtiff	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	10.19.45.1	Not vulnerable	LIN1018-5090
863	CVE-2019-17545	HIGH	CRITICAL	GDAL through 3.0.1 has a poolDestroy double free in OGRExpatRealloc in ogr/ogr_expat.cpp when the 10MB threshold is exceeded.	gdal	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-9185
864	CVE-2019-17544	MEDIUM	CRITICAL	libaspell.a in GNU Aspell before 0.60.8 has a stack-based buffer over-read in acommon::unescape in common/getdata.cpp via an isolated \ character.	aspell	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-5092
865	CVE-2019-17543	MEDIUM	HIGH	LZ4 before 1.9.2 has a heap-based buffer overflow in LZ4_write32 (related to LZ4_compress_destSize), affecting applications that call LZ4_compress_fast with a large input. (This issue can also lead to data corruption.) NOTE: the vendor states only a few specific / uncommon usages of the API are at risk.	lz4	Unchanged	Not vulnerable	Not vulnerable	Investigate	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-5091
866	CVE-2019-17542	HIGH	CRITICAL	FFmpeg before 4.2 has a heap-based buffer overflow in vqa_decode_chunk because of an out-of-array access in vqa_decode_init in libavcodec/vqavideo.c.	ffmpeg	Unchanged	Won't Fix	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5096
867	CVE-2019-17541	MEDIUM	HIGH	ImageMagick before 7.0.8-55 has a use-after-free in DestroyStringInfo in MagickCore/string.c because the error manager is mishandled in coders/jpeg.c.	imagemagick	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5094
868	CVE-2019-17540	MEDIUM	HIGH	ImageMagick before 7.0.8-54 has a heap-based buffer overflow in ReadPSInfo in coders/ps.c.	imagemagick	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5095

	A	B	C	D	E	F	G	H	I	J	K	L	M
869	CVE-2019-17539	HIGH	CRITICAL	In FFmpeg before 4.2, avcodec_open2 in libavcodec/utils.c allows a NULL pointer dereference and possibly unspecified other impact when there is no valid close function pointer.	ffmpeg	Unchanged	Won't Fix	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5097
870	CVE-2019-17514	MEDIUM	HIGH	library/glob.html in the Python 2 and 3 documentation before 2016 has potentially misleading information about whether sorting occurs, as demonstrated by irreproducible cancer-research results. NOTE: the effects of this documentation cross application domains, and thus it is likely that security-relevant code elsewhere is affected. This issue is not a Python implementation bug, and there are no reports that NMR researchers were specifically relying on library/glob.html. In other words, because the older documentation stated finds all the pathnames matching a specified pattern according to the rules used by the Unix shell, one might have incorrectly inferred that the sorting that occurs in a Unix shell also occurred for glob.glob. There is a workaround in newer versions of Willoughby nmr-data_compilation-p2.py and nmr-data_compilation-p3.py, which call sort() directly.	python	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-5189
871	CVE-2019-17498	MEDIUM	HIGH	In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, enabling an attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server.	libssh2	Unchanged	8.0.0.32	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5153
872	CVE-2019-17451	MEDIUM	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an integer overflow leading to a SEGV in _bfd_dwarf2_find_nearest_line in dwarf2.c, as demonstrated by nm.	binutils	Unchanged	Vulnerable	Vulnerable	10.17.41.20	10.18.44.12	10.19.45.6	10.20.3.0	LIN1018-5080
873	CVE-2019-17450	MEDIUM	MEDIUM	find_abstract_instance in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32, allows remote attackers to cause a denial of service (infinite recursion and application crash) via a crafted ELF file.	binutils	Unchanged	Vulnerable	Vulnerable	10.17.41.20	10.18.44.12	10.19.45.6	10.20.3.0	LIN1018-5081
874	CVE-2019-17420	MEDIUM	MEDIUM	In OISF LibHTP before 0.5.31, as used in Suricata 4.1.4 and other products, an HTTP protocol parsing error causes the http_header signature to not alert on a response with a single \r\n ending.	suricata	Unchanged	Investigate	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5083
875	CVE-2019-17382	MEDIUM	CRITICAL	An issue was discovered in zabbix.php?action=dashboard.view&dashboardid=1 in Zabbix through 4.4. An attacker can bypass the login page and access the dashboard page, and then create a Dashboard, Report, Screen, or Map without any Username/Password (i.e., anonymously). All created elements (Dashboard/Report/Screen/Map) are accessible by other users and by an admin.	zabbix	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-5070
876	CVE-2019-17371	Medium	MEDIUM	libpng 1.6.37 has memory leaks in png_malloc_warn and png_create_info_struct.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5065
877	CVE-2019-17361	MEDIUM	CRITICAL	In SaltStack Salt through 2019.2.0, the salt-api NEST API with the ssh client enabled is vulnerable to command injection. This allows an unauthenticated attacker with network access to the API endpoint to execute arbitrary code on the salt-api host.	salt	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3955
878	CVE-2019-17351	Medium	MEDIUM	An issue was discovered in drivers/xen/balloon.c in the Linux kernel before 5.2.3, as used in Xen through 4.12.x, allowing guest OS users to cause a denial of service because of unrestricted resource consumption during the mapping of guest memory, aka CID-6ef36ab967c7.	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5048
879	CVE-2019-17266	High	CRITICAL	libsoup from versions 2.65.1 until 2.68.1 have a heap-based buffer over-read because soup_ntlm_parse_challenge() in soup-auth-ntlm.c does not properly check an NTLM message's length before proceeding with a memcpy.	libsoup	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4977
880	CVE-2019-17185	MEDIUM	HIGH	In FreeRADIUS 3.0.x before 3.0.20, the EAP-pwd module used a global OpenSSL BN_CTX instance to handle all handshakes. This mean multiple threads use the same BN_CTX instance concurrently, resulting in crashes when concurrent EAP-pwd handshakes are initiated. This can be abused by an adversary as a Denial-of-Service (DoS) attack.	freeradius	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4160
881	CVE-2019-17178	Medium	HIGH	HuffmanTree_makeFromFrequencies in lodepng.c in LodePNG through 2019-09-28, as used in WinPR in FreeRDP and other products, has a memory leak because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.	freerdp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5049
882	CVE-2019-17177	Medium	HIGH	libfreerdp/codec/region.c in FreeRDP through 1.1.x and 2.x through 2.0.0-rc4 has memory leaks because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.	freerdp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5050
883	CVE-2019-17133	High	CRITICAL	In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/wireless/wext-sme.c does not reject a long SSID IE, leading to a Buffer Overflow.	linux	Unchanged	8.0.0.32	9.0.0.24	10.17.41.19	10.18.44.13	10.19.45.1	10.20.3.0	LIN1018-4978
884	CVE-2019-17075	High	HIGH	An issue was discovered in write_tpt_entry in drivers/infiniband/hw/cxgb4/mem.c in the Linux kernel through 5.3.2. The cxgb4 driver is directly calling dma_map_single (a DMA function) from a stack variable. This could allow an attacker to trigger a Denial of Service, exploitable if this driver is used on an architecture for which this stack/DMA interaction has security relevance.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.2	10.20.3.0	LIN1018-5039
885	CVE-2019-17056	Low	LOW	llcp_sock_create in net/nfc/llcp_sock.c in the AF_NFC network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-3a359798b176.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.1	Not vulnerable	LIN1018-5038

	A	B	C	D	E	F	G	H	I	J	K	L	M
886	CVE-2019-17055	Low	LOW	base_sock_create in drivers/isdn/mISDN/socket.c in the AF_ISDN network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-b91ee4aa2a21.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.1	Not vulnerable	LIN1018-5037
887	CVE-2019-17054	Low	LOW	atalk_create in net/appletalk/ddp.c in the AF_APPLETALK network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-6cc03e8aa36c.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.1	Not vulnerable	LIN1018-5036
888	CVE-2019-17053	Low	LOW	ieee802154_create in net/ieee802154/socket.c in the AF_IEEE802154 network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-e69dbd4619e7.	linux	Unchanged	8.0.0.32	9.0.0.24	10.17.41.19	10.18.44.13	10.19.45.1	Not vulnerable	LIN1018-5035
889	CVE-2019-17052	Low	LOW	ax25_create in net/ax25/af_ax25.c in the AF_AX25 network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-0614e2b73768.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5034
890	CVE-2019-17041	HIGH	CRITICAL	An issue was discovered in Rsyslog v8.1908.0. contrib/pmaixforwardedfrom/pmaixforwardedfrom.c has a heap overflow in the parser for AIX log messages. The parser tries to locate a log message delimiter (in this case, a space or a colon) but fails to account for strings that do not satisfy this constraint. If the string does not match, then the variable lenMsg will reach the value zero and will skip the sanity check that detects invalid log messages. The message will then be considered valid, and the parser will eat up the nonexistent colon delimiter. In doing so, it will decrement lenMsg, a signed integer, whose value was zero and now becomes minus one. The following step in the parser is to shift left the contents of the message. To do this, it will call memmove with the right pointers to the target and destination strings, but the lenMsg will now be interpreted as a huge value, causing a heap overflow.	rsyslog	Unchanged	Not vulnerable	9.0.0.24	10.17.41.20	10.18.44.11	10.19.45.1	Not vulnerable	LIN1018-5087
891	CVE-2019-17040	High	CRITICAL	contrib/pmdb2diag/pmdb2diag.c in Rsyslog v8.1908.0 allows out-of-bounds access because the level length is mishandled.	rsyslog	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5051
892	CVE-2019-16995	High	HIGH	In the Linux kernel before 5.0.3, a memory leak exits in hsr_dev_finalize() in net/hsr/hsr_device.c if hsr_add_port fails to add a port, which may cause denial of service, aka CID-6caabe7f197d.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5044
893	CVE-2019-16994	High	HIGH	In the Linux kernel before 5.0, a memory leak exists in sit_init_net() in net/ipv6/sit.c when register_netdev() fails to register sitn->fb_tunnel_dev, which may cause denial of service, aka CID-07f12b26e21a.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5043
894	CVE-2019-16935	Medium	MEDIUM	The documentation XML-RPC server in Python through 2.7.16, 3.x through 3.6.9, and 3.7.x through 3.7.4 has XSS via the server_title field. This occurs in Lib/DocXMLRPCServer.py in Python 2.x, and in Lib/xmlrpc/server.py in Python 3.x. If set_server_title is called with untrusted input, arbitrary JavaScript can be delivered to clients that visit the http URL for this server.	python	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.6	Not vulnerable	LIN1018-5042
895	CVE-2019-16921	Medium	HIGH	In the Linux kernel before 4.17, hns_roce_alloc_ucontext in drivers/infiniband/hw/hns/hns_roce_main.c does not initialize the resp data structure, which might allow attackers to obtain sensitive information from kernel stack memory, aka CID-df7e40425813.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5032
896	CVE-2019-16910	Low	MEDIUM	Arm Mbed TLS before 2.19.0 and Arm Mbed Crypto before 2.0.0, when deterministic ECDSA is enabled, use an RNG with insufficient entropy for blinding, which might allow an attacker to recover a private key via side-channel attacks if a victim signs the same message many times. (For Mbed TLS, the fix is also available in versions 2.7.12 and 2.16.3.)	mbedtls	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5033
897	CVE-2019-16905	MEDIUM	HIGH	OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and remote code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-5069
898	CVE-2019-16884	Medium	HIGH	runc through 1.0.0-rc8, as used in Docker through 19.03.2-ce and other products, allows AppArmor restriction bypass because libcontainer/rootfs_linux.go incorrectly checks mount targets, and thus a malicious Docker image can mount over a /proc directory.	runc-docker	Unchanged	Not vulnerable	Not vulnerable	Investigate	Investigate	Investigate	10.20.3.0	LIN1018-5041
899	CVE-2019-16748	High	CRITICAL	In wolfSSL through 4.1.0, there is a missing sanity check of memory accesses in parsing ASN.1 certificate data while handshaking. Specifically, there is a one-byte heap-based buffer over-read in CheckCertSignature_ex in wolfcrypt/src/asn.c.	wolfssl	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5031
900	CVE-2019-16746	High	CRITICAL	An issue was discovered in net/wireless/nl80211.c in the Linux kernel through 5.2.17. It does not check the length of variable elements in a beacon head, leading to a buffer overflow.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-5030
901	CVE-2019-16714	Medium	HIGH	In the Linux kernel before 5.2.14, rds6_inc_info_copy in net/rds/recv.c allows attackers to obtain sensitive information from kernel stack memory because tos and flags fields are not initialized.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5029
902	CVE-2019-16713	Medium	MEDIUM	ImageMagick 7.0.8-43 has a memory leak in coders/dot.c, as demonstrated by PingImage in MagickCore/constitute.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5027
903	CVE-2019-16712	Medium	MEDIUM	ImageMagick 7.0.8-43 has a memory leak in Huffman2DEncodeImage in coders/ps3.c, as demonstrated by WritePS3Image.	imagemagick	Unchanged	8.0.0.31	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5026
904	CVE-2019-16711	Medium	MEDIUM	ImageMagick 7.0.8-40 has a memory leak in Huffman2DEncodeImage in coders/ps2.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5025

	A	B	C	D	E	F	G	H	I	J	K	L	M
905	CVE-2019-16710	Medium	MEDIUM	ImageMagick 7.0.8-35 has a memory leak in coders/dot.c, as demonstrated by AcquireMagickMemory in MagickCore/memory.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5024
906	CVE-2019-16709	Medium	MEDIUM	ImageMagick 7.0.8-35 has a memory leak in coders/dps.c, as demonstrated by XCreateImage.	imagemagick	Unchanged	8.0.0.31	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5023
907	CVE-2019-16708	Medium	MEDIUM	ImageMagick 7.0.8-35 has a memory leak in magick/xwindow.c, related to XCreateImage.	imagemagick	Unchanged	8.0.0.31	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5022
908	CVE-2019-16707	Medium	MEDIUM	Hunspell 1.7.0 has an invalid read operation in SuggestMgr::leftcommonsubstring in suggestmgr.cxx.	hunspell	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5052
909	CVE-2019-16413	Medium	HIGH	An issue was discovered in the Linux kernel before 5.0.4. The 9p filesystem did not protect i_size_write() properly, which causes an i_size_read() infinite loop and denial of service on SMP systems.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4952
910	CVE-2019-16411	High	CRITICAL	An issue was discovered in Suricata 4.1.4. By sending multiple IPv4 packets that have invalid IPv4Options, the function IPV4OptValidateTimestamp in decode-ipv4.c tries to access a memory region that is not allocated. There is a check for o->len < 5 (corresponding to 2 bytes of header and 3 bytes of data). Then, flag = *(o->data + 3) places one beyond the 3 bytes, because the code should have been flag = *(o->data + 1) instead.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5021
911	CVE-2019-16410	Medium	CRITICAL	An issue was discovered in Suricata 4.1.4. By sending multiple fragmented IPv4 packets, the function Defrag4Reassemble in defrag.c tries to access a memory region that is not allocated, because of a lack of header_len checking.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5020
912	CVE-2019-16319	HIGH	HIGH	In Wireshark 3.0.0 to 3.0.3 and 2.6.0 to 2.6.10, the Gryphon dissector could go into an infinite loop. This was addressed in plugins/epan/gryphon/packet-gryphon.c by checking for a message length of zero.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4927
913	CVE-2019-16279	MEDIUM	HIGH	A memory error in the function SSL_accept in nostromo nhttpd through 1.9.6 allows an attacker to trigger a denial of service via a crafted HTTP request.	nostromo	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5186
914	CVE-2019-16278	HIGH	CRITICAL	Directory Traversal in the function http_verify in nostromo nhttpd through 1.9.6 allows an attacker to achieve remote code execution via a crafted HTTP request.	nostromo	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5188
915	CVE-2019-16276	Medium	HIGH	Go before 1.12.10 and 1.13.x before 1.13.1 allow HTTP Request Smuggling.	go	Unchanged	Not vulnerable	Won't Fix	10.17.41.19	10.18.44.12	10.19.45.6	10.20.3.0	LIN1018-5028
916	CVE-2019-16275	Low	MEDIUM	hostapd before 2.10 and wpa_supplicant before 2.10 allow an incorrect indication of disconnection in certain situations because source address validation is mishandled. This is a denial of service that should have been prevented by PMF (aka management frame protection). The attacker must send a crafted 802.11 frame from a location that is within the 802.11 communications range.	hostapd&wpa-supplicant	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	10.19.45.2	Investigate	LIN1018-4929
917	CVE-2019-16255	HIGH	CRITICAL	Ruby through 2.4.7, 2.5.x through 2.5.6, and 2.6.x through 2.6.4 allows code injection if the first argument (aka the command argument) to Shell#[] or Shell#test in lib/shell.rb is untrusted data. An attacker can exploit this to call an arbitrary Ruby method.	ruby	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3655
918	CVE-2019-16254	MEDIUM	MEDIUM	Ruby through 2.4.7, 2.5.x through 2.5.6, and 2.6.x through 2.6.4 allows HTTP Response Splitting. If a program using WEBrick inserts untrusted input into the response header, an attacker can exploit it to insert a newline character to split a header, and inject malicious content to deceive clients. NOTE: this issue exists because of an incomplete fix for CVE-2017-17742, which addressed the CRLF vector, but did not address an isolated CR or an isolated LF.	ruby	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3656
919	CVE-2019-16249	High	CRITICAL	OpenCV 4.1.1 has an out-of-bounds read in hal_baseline::v_load in core/hal/intrin_sse.hpp when called from computeSSDMeanNorm in modules/video/src/dis_flow.cpp.	opencv	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4928
920	CVE-2019-16239	High	CRITICAL	process_http_response in OpenConnect before 8.05 has a Buffer Overflow when a malicious server uses HTTP chunked encoding with crafted chunk sizes.	openconnect	Unchanged	Not vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5054
921	CVE-2019-16234	High	HIGH	drivers/net/wireless/intel/iwlwifi/pcie/trans.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-4919
922	CVE-2019-16233	High	HIGH	drivers/scsi/qla2xxx/qla_os.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	Not vulnerable	Not vulnerable	LIN1018-4920
923	CVE-2019-16232	High	HIGH	drivers/net/wireless/marvell/libertas/if_sdio.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.	linux	Unchanged	Not vulnerable	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.5	Not vulnerable	LIN1018-4921
924	CVE-2019-16231	High	HIGH	drivers/net/fjes/fjes_main.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.	linux	Unchanged	Not vulnerable	9.0.0.25	10.17.41.19	10.18.44.14	Not vulnerable	Not vulnerable	LIN1018-4922
925	CVE-2019-16230	High	HIGH	drivers/gpu/drm/radeon/radeon_display.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-4923
926	CVE-2019-16229	High	HIGH	drivers/gpu/drm/amd/amdkfd/kfd_interrupt.c in the Linux kernel 5.2.14 does not check the alloc_workqueue return value, leading to a NULL pointer dereference.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	Not vulnerable	Not vulnerable	LIN1018-4924
927	CVE-2019-16201	HIGH	HIGH	WEBrick::HTTPAuth::DigestAuth in Ruby through 2.4.7, 2.5.x through 2.5.6, and 2.6.x through 2.6.4 has a regular expression Denial of Service cause by looping/backtracking. A victim must expose a WEBrick server that uses DigestAuth to the Internet or a untrusted network.	ruby	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3663
928	CVE-2019-16168	Medium	HIGH	In SQLite through 3.29.0, whereLoopAddBtreeIndex in sqlite3.c can crash a browser or other application because of missing validation of a sqlite_stat1 sz field, aka a severe division by zero in the query planner.	sqlite	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.6	Not vulnerable	LIN1018-4880
929	CVE-2019-16167	Medium	MEDIUM	sysstat before 12.1.6 has memory corruption due to an Integer Overflow in remap_struct() in sa_common.c.	sysstat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.11	10.19.45.6	Not vulnerable	LIN1018-4879

	A	B	C	D	E	F	G	H	I	J	K	L	M
930	CVE-2019-16089	High	CRITICAL	An issue was discovered in the Linux kernel through 5.2.13. nbd_genl_status in drivers/block/nbd.c does not check the nla_nest_start_noflag return value.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-4863
931	CVE-2019-16056	Medium	HIGH	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.	python	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	10.19.45.6	Not vulnerable	LIN1018-4865
932	CVE-2019-15961	HIGH	MEDIUM	A vulnerability in the email parsing module Clam AntiVirus (ClamAV) Software versions 0.102.0, 0.101.4 and prior could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to inefficient MIME parsing routines that result in extremely long scan times of specially formatted email files. An attacker could exploit this vulnerability by sending a crafted email file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process to scan the crafted email file indefinitely, resulting in a denial of service condition.	clamav	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3956
933	CVE-2019-15946	High	CRITICAL	OpenSC before 0.20.0-rc1 has an out-of-bounds access of an ASN.1 Octet string in asn1_decode_entry in libopensc/asn1.c.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4931
934	CVE-2019-15945	High	CRITICAL	OpenSC before 0.20.0-rc1 has an out-of-bounds access of an ASN.1 Bitstring in decode_bit_string in libopensc/asn1.c.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4930
935	CVE-2019-15942	Medium	HIGH	FFmpeg through 4.2 has a Conditional jump or move depends on uninitialised value issue in h2645_parse because alloc_rbsp_buffer in libavcodec/h2645_parse.c mishandles rbsp_buffer.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4859
936	CVE-2019-15939	Medium	HIGH	An issue was discovered in OpenCV 4.1.0. There is a divide-by-zero error in cv::HOGDescriptor::getDescriptorSize in modules/objdetect/src/hog.cpp.	opencv	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4860
937	CVE-2019-15927	High	HIGH	An issue was discovered in the Linux kernel before 4.20.2. An out-of-bounds access exists in the function build_audio_procunit in the file sound/usb/mixer.c.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4853
938	CVE-2019-15926	High	CRITICAL	An issue was discovered in the Linux kernel before 5.2.3. Out of bounds access exists in the functions ath6kl_wmi_pstream_timeout_event_rx and ath6kl_wmi_cac_event_rx in the file drivers/net/wireless/ath/ath6kl/wmi.c.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4852
939	CVE-2019-15925	High	HIGH	An issue was discovered in the Linux kernel before 5.2.3. An out of bounds access exists in the function hclge_tm_schd_mode_vnet_base_cfg in the file drivers/net/ethernet/hisilicon/hns3/hns3pf/hclge_tm.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4851
940	CVE-2019-15924	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.0.11. fm10k_init_module in drivers/net/ethernet/intel/fm10k/fm10k_main.c has a NULL pointer dereference because there is no -ENOMEM upon an alloc_workqueue failure.	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4850
941	CVE-2019-15923	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a cd data structure if alloc_disk fails in drivers/block/paride/pf.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4849
942	CVE-2019-15922	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a pf data structure if alloc_disk fails in drivers/block/paride/pf.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4848
943	CVE-2019-15921	Medium	HIGH	An issue was discovered in the Linux kernel before 5.0.6. There is a memory leak issue when idr_alloc() fails in genl_register_family() in net/netlink/genetlink.c.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4847
944	CVE-2019-15920	High	HIGH	An issue was discovered in the Linux kernel before 5.0.10. SMB2_read in fs/cifs/smb2pdu.c has a use-after-free. NOTE: this was not fixed correctly in 5.0.10; see the 5.0.11 ChangeLog, which documents a memory leak.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4846
945	CVE-2019-15919	High	HIGH	An issue was discovered in the Linux kernel before 5.0.10. SMB2_write in fs/cifs/smb2pdu.c has a use-after-free.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4845
946	CVE-2019-15918	High	HIGH	An issue was discovered in the Linux kernel before 5.0.10. SMB2_negotiate in fs/cifs/smb2pdu.c has an out-of-bounds read because data structures are incompletely updated after a change from smb30 to smb21.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4844
947	CVE-2019-15917	High	HIGH	An issue was discovered in the Linux kernel before 5.0.5. There is a use-after-free issue when hci_uart_register_dev() fails in hci_uart_set_proto() in drivers/bluetooth/hci_ldisc.c.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4843
948	CVE-2019-15916	High	HIGH	An issue was discovered in the Linux kernel before 5.0.1. There is a memory leak in register_queue_kobjects() in net/core/net-sysfs.c, which will cause denial of service.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4842
949	CVE-2019-15902	High	CRITICAL	A backporting error was discovered in the Linux stable/longterm kernel 4.4.x through 4.4.190, 4.9.x through 4.9.190, 4.14.x through 4.14.141, 4.19.x through 4.19.69, and 5.2.x through 5.2.11. Misuse of the upstream x86/ptrace: Fix possible spectre-v1 in ptrace_get_debugreg() commit reintroduced the Spectre vulnerability that it aimed to eliminate. This occurred because the backport process depends on cherry picking specific commits, and because two (correctly ordered) code lines were swapped.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4841
950	CVE-2019-15890	Medium	HIGH	libslirp 4.0.0, as used in QEMU 4.1.0, has a use-after-free in ip_reass in ip_input.c.	qemu	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4864
951	CVE-2019-15845	HIGH	CRITICAL	Ruby through 2.4.7, 2.5.x through 2.5.6, and 2.6.x through 2.6.4 mishandles path checking within File.fnmatch functions.	ruby	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.2	Not vulnerable	LIN1019-3657
952	CVE-2019-15807	HIGH	HIGH	In the Linux kernel before 5.1.13, there is a memory leak in drivers/scsi/libsas/sas_expander.c when SAS expander discovery fails. This will cause a BUG and denial of service.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4788

	A	B	C	D	E	F	G	H	I	J	K	L	M
953	CVE-2019-15785	HIGH	CRITICAL	FontForge through 20190801 has a buffer overflow in PrefsUI_LoadPrefs in prefs.c.	fontforge	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4807
954	CVE-2019-15718	Low	MEDIUM	In systemd 240, bus_open_system_watch_bind_with_description in shared/bus-util.c (as used by systemd-resolved to connect to the system D-Bus instance), calls sd_bus_set_trusted, which disables access controls for incoming D-Bus messages. An unprivileged user can exploit this by executing D-Bus methods that should be restricted to privileged users, in order to change the system's DNS resolver settings.	systemd	Unchanged	Investigate	Investigate	Investigate	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4854
955	CVE-2019-15717	HIGH	CRITICAL	Irssi 1.2.x before 1.2.2 has a use-after-free if the IRC server sends a double CAP.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4787
956	CVE-2019-15699	Medium	CRITICAL	An issue was discovered in app-layer-ssl.c in Suricata 4.1.4. Upon receiving a corrupted SSLv3 (TLS 1.2) packet, the parser function TLSDecodeHSHelloExtensions tries to access a memory region that is not allocated, because the expected length of HSHelloExtensions does not match the real length of the HSHelloExtensions part of the packet.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5019
957	CVE-2019-15695	MEDIUM	HIGH	TigerVNC version prior to 1.10.1 is vulnerable to stack buffer overflow, which could be triggered from CMsgReader::readSetCursor. This vulnerability occurs due to insufficient sanitization of PixelFormat. Since remote attacker can choose offset from start of the buffer to start writing his values, exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.	tigervnc	Unchanged	Not vulnerable	Investigate	10.17.41.20	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3873
958	CVE-2019-15694	MEDIUM	HIGH	TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow, which could be triggered from DecodeManager::decodeRect. Vulnerability occurs due to the signdness error in processing MemOutStream. Exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.	tigervnc	Unchanged	Not vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3874
959	CVE-2019-15693	MEDIUM	HIGH	TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow, which occurs in TightDecoder::FilterGradient. Exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.	tigervnc	Unchanged	Not vulnerable	Investigate	10.17.41.20	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3875
960	CVE-2019-15692	MEDIUM	HIGH	TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow. Vulnerability could be triggered from CopyRectDecoder due to incorrect value checks. Exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.	tigervnc	Unchanged	Not vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3876
961	CVE-2019-15691	MEDIUM	HIGH	TigerVNC version prior to 1.10.1 is vulnerable to stack use-after-return, which occurs due to incorrect usage of stack memory in ZRLEDecoder. If decoding routine would throw an exception, ZRLEDecoder may try to access stack variable, which has been already freed during the process of stack unwinding. Exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.	tigervnc	Unchanged	Not vulnerable	Investigate	10.17.41.20	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3877
962	CVE-2019-15681	MEDIUM	HIGH	LibVNC commit before d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a contains a memory leak (CWE-655) in VNC server code, which allow an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appear to be exploitable via network connectivity. These vulnerabilities have been fixed in commit d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a.	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5175
963	CVE-2019-15666	HIGH	HIGH	An issue was discovered in the Linux kernel before 5.0.19. There is an out-of-bounds array access in __xfrm_policy_unlink, which will cause denial of service, because verify_newpolicy_info in net/xfrm/xfrm_user.c mishandles directory validation.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4774
964	CVE-2019-15651	HIGH	CRITICAL	wolfSSL 4.1.0 has a one-byte heap-based buffer over-read in DecodeCertExtensions in wolfcrypt/src/asn.c because reading the ASN_BOOLEAN byte is mishandled for a crafted DER certificate in GetLength_ex.	wolfssl	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4771
965	CVE-2019-15642	MEDIUM	HIGH	rpc.cgi in Webmin through 1.920 allows authenticated Remote Code Execution via a crafted object name because unserialise_variable makes an eval call. NOTE: the Webmin_Servers_Index documentation states RPC can be used to run any command or modify any file on a server, which is why access to it must not be granted to un-trusted Webmin users.	webmin	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4769
966	CVE-2019-15641	MEDIUM	MEDIUM	xmlrpc.cgi in Webmin through 1.930 allows authenticated XXE attacks. By default, only root, admin, and sysadm can access xmlrpc.cgi.	webmin	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4770
967	CVE-2019-1563	Medium	LOW	In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).	openssl	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4901

	A	B	C	D	E	F	G	H	I	J	K	L	M
968	CVE-2019-15606	HIGH	CRITICAL	Including trailing white space in HTTP header values in Nodejs 10, 12, and 13 causes bypass of authorization based on header value comparisons	nodejs	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4015
969	CVE-2019-15605	HIGH	CRITICAL	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	nodejs	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4016
970	CVE-2019-15604	MEDIUM	HIGH	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	nodejs	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4017
971	CVE-2019-1559	Medium	MEDIUM	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable non-stitched ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).	openssl	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3653
972	CVE-2019-15538	HIGH	HIGH	An issue was discovered in xfs_setattr_nonsize in fs/xfs/xfs_iops.c in the Linux kernel through 5.2.9. XFS partially wedges when a chgrp fails on account of being out of disk quota. xfs_setattr_nonsize is failing to unlock the ILOCK after the xfs_qm_vop_chown_reserve call fails. This is primarily a local DoS attack vector, but it might result as well in remote DoS if the XFS filesystem is exported for instance via NFS.	linux	Unchanged	Not vulnerable	Vulnerable	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4766
973	CVE-2019-1552	LOW	LOW	OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).	openssl	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4574
974	CVE-2019-1551	MEDIUM	MEDIUM	There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e-dev (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u-dev (Affected 1.0.2-1.0.2t).	openssl	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	10.20.3.0	LIN1019-3726
975	CVE-2019-15505	High	CRITICAL	drivers/media/usb/dvb-usb/technisat-usb2.c in the Linux kernel through 5.2.9 has an out-of-bounds read via crafted USB device traffic (which may be remote via usbip or usbredir).	linux	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	Not vulnerable	Not vulnerable	LIN1018-4767
976	CVE-2019-15504	High	CRITICAL	drivers/net/wireless/rsi/rsi_91x_usb.c in the Linux kernel through 5.2.9 has a Double Free via crafted USB device traffic (which may be remote via usbip or usbredir).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	Not vulnerable	Not vulnerable	LIN1018-4768
977	CVE-2019-1549	Medium	MEDIUM	OpenSSL 1.1.1 introduced a rewritten random number generator (RNG). This was intended to include protection in the event of a fork() system call in order to ensure that the parent and child processes did not share the same RNG state. However this protection was not being used in the default case. A partial mitigation for this issue is that the output from a high precision timer is mixed into the RNG state so the likelihood of a parent and child process sharing state is significantly reduced. If an application already calls OPENSSL_init_crypto() explicitly using OPENSSL_INIT_ATFORK then this problem does not occur at all. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c).	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4902

	A	B	C	D	E	F	G	H	I	J	K	L	M
978	CVE-2019-1547	Low	MEDIUM	Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).	openssl	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4903
979	CVE-2019-1543	Medium	HIGH	ChaCha20-Poly1305 is an AEAD cipher, and requires a unique nonce input for every encryption operation. RFC 7539 specifies that the nonce value (IV) should be 96 bits (12 bytes). OpenSSL allows a variable nonce length and front pads the nonce with 0 bytes if it is less than 12 bytes. However it also incorrectly allows a nonce to be set of up to 16 bytes. In this case only the last 12 bytes are significant and any additional leading bytes are ignored. It is a requirement of using this cipher that nonce values are unique. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. If an application changes the default nonce length to be longer than 12 bytes and then makes a change to the leading bytes of the nonce expecting the new value to be a new unique nonce then such an application could inadvertently encrypt messages with a reused nonce. Additionally the ignored bytes in a long nonce are not covered by the integrity guarantee of this cipher. Any application that relies on the integrity of these ignored leading bytes of a long nonce may be further affected. Any OpenSSL internal use of this cipher, including in SSL/TLS, is safe because no such use sets such a long nonce value. However user applications that use this cipher directly and set a non-default nonce length to be longer than 12 bytes may be vulnerable. OpenSSL versions 1.1.1 and 1.1.0 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1c-dev (Affected 1.1.1-1.1.1b). Fixed in OpenSSL 1.1.0k-dev (Affected 1.1.0-1.1.0j).	openssl	Unchanged	Not vulnerable	Not vulnerable	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3781
980	CVE-2019-15296	Medium	HIGH	An issue was discovered in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The faad_resetbits function in libfaad/bits.c is affected by a buffer overflow vulnerability. The number of bits to be read is determined by ld->buffer_size - words*4, cast to uint32. If ld->buffer_size - words*4 is negative, a buffer overflow is later performed via getdword_n(&ld->start[words], ld->bytes_left).	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4808
981	CVE-2019-15292	High	CRITICAL	An issue was discovered in the Linux kernel before 5.0.9. There is a use-after-free in atalk_proc_exit, related to net/appletalk/atalk_proc.c, net/appletalk/ddp.c, and net/appletalk/sysctl_net_atalk.c.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4747
982	CVE-2019-15291	Medium	MEDIUM	An issue was discovered in the Linux kernel through 5.2.9. There is a NULL pointer dereference caused by a malicious USB device in the flexcop_usb_probe function in the drivers/media/usb/b2c2/flexcop-usb.c driver.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-4732
983	CVE-2019-15290	Medium	MEDIUM	An issue was discovered in the Linux kernel through 5.2.9. There is a NULL pointer dereference caused by a malicious USB device in the ath6kl_usb_alloc_urb_from_pipe function in the drivers/net/wireless/ath/ath6kl/usb.c driver.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4733
984	CVE-2019-15239	HIGH	HIGH	In the Linux kernel, a certain net/ipv4/tcp_output.c change, which was properly incorporated into 4.16.12, was incorrectly backported to the earlier longterm kernels, introducing a new vulnerability that was potentially more severe than the issue that was intended to be fixed by backporting. Specifically, by adding to a write queue between disconnection and re-connection, a local attacker can trigger multiple use-after-free conditions. This can result in a kernel crash, or potentially in privilege escalation. NOTE: this affects (for example) Linux distributions that use 4.9.x longterm kernels before 4.9.190 or 4.14.x longterm kernels before 4.14.139.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4734
985	CVE-2019-15232	High	CRITICAL	Live555 before 2019.08.16 has a Use-After-Free because GenericMediaServer::createNewClientSessionWithId can generate the same client session ID in succession, which is mishandled by the MPEG1or2 and Matroska file demultiplexors.	live555	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4737
986	CVE-2019-15223	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/line6/driver.c driver.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4727
987	CVE-2019-15222	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.2.8. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/helper.c (motu_microbookii) driver.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4726
988	CVE-2019-15221	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.1.17. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/line6/pcm.c driver.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4725

	A	B	C	D	E	F	G	H	I	J	K	L	M
989	CVE-2019-15220	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.2.1. There is a use-after-free caused by a malicious USB device in the drivers/net/wireless/intersil/p54/p54usb.c driver.	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4724
990	CVE-2019-15219	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the drivers/usb/misc/sisusbvga/sisusb.c driver.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4723
991	CVE-2019-15218	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the drivers/media/usb/siano/smsusb.c driver.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4722
992	CVE-2019-15217	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.2.3. There is a NULL pointer dereference caused by a malicious USB device in the drivers/media/usb/zr364xx/zr364xx.c driver.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4721
993	CVE-2019-15216	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.0.14. There is a NULL pointer dereference caused by a malicious USB device in the drivers/usb/misc/yurex.c driver.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4720
994	CVE-2019-15215	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/usb/cpia2/cpia2_usb.c driver.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4719
995	CVE-2019-15214	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.0.10. There is a use-after-free in the sound subsystem because card disconnection causes certain data structures to be deleted too early. This is related to sound/core/init.c and sound/core/info.c.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4718
996	CVE-2019-15213	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.2.3. There is a use-after-free caused by a malicious USB device in the drivers/media/usb/dvb-usb/dvb-usb-init.c driver.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4717
997	CVE-2019-15212	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.1.8. There is a double-free caused by a malicious USB device in the drivers/usb/misc/rio500.c driver.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4716
998	CVE-2019-15211	Medium	MEDIUM	An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/v4l2-core/v4l2-dev.c driver because drivers/media/radio/radio-raremono.c does not properly allocate memory.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4715
999	CVE-2019-15167			Tcpdump is vulnerable to a buffer overflow, caused by improper bounds checking by the lmp_print_data_link_subobjs function in print-lmp.c. By sending specially-crafted data, a remote attacker could overflow a buffer and cause the application to crash.	tcpdump	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN1019-4137
1000	CVE-2019-15166	High	CRITICAL	lmp_print_data_link_subobjs() in print-lmp.c in tcpdump before 4.9.3 lacks certain bounds checks.	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-5018
1001	CVE-2019-15165	Medium	MEDIUM	sf-pcapng.c in libpcap before 1.9.1 does not properly validate the PHB header length before allocating memory.	libpcap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5017
1002	CVE-2019-15164	Medium	MEDIUM	rpcapd/daemon.c in libpcap before 1.9.1 allows SSRF because a URL may be provided as a capture source.	libpcap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5016
1003	CVE-2019-15163	Medium	HIGH	rpcapd/daemon.c in libpcap before 1.9.1 allows attackers to cause a denial of service (NULL pointer dereference and daemon crash) if a crypt() call fails.	libpcap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5015
1004	CVE-2019-15161	Medium	MEDIUM	rpcapd/daemon.c in libpcap before 1.9.1 mishandles certain length values because of reuse of a variable. This may open up an attack vector involving extra data at the end of a request.	libpcap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-5013
1005	CVE-2019-15141	Medium	MEDIUM	WriteTIFFImage in coders/tiff.c in ImageMagick 7.0.8-43 Q16 allows attackers to cause a denial-of-service (application crash resulting from a heap-based buffer over-read) via a crafted TIFF image file, related to TIFFRewriteDirectory, TIFFWriteDirectory, TIFFWriteDirectorySec, and TIFFWriteDirectoryTagColormap in tif_dirwrite.c of LibTIFF. NOTE: this occurs because of an incomplete fix for CVE-2019-11597.	imagemagick	Unchanged	Investigate	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4685
1006	CVE-2019-15140	Medium	HIGH	coders/mat.c in ImageMagick 7.0.8-43 Q16 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact by crafting a Matlab image file that is mishandled in ReadImage in MagickCore/constitute.c.	imagemagick	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4686
1007	CVE-2019-15139	Medium	MEDIUM	The XWD image (X Window System window dumping file) parsing component in ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (application crash resulting from an out-of-bounds Read) in ReadXWDImage in coders/xwd.c by crafting a corrupted XWD image file, a different vulnerability than CVE-2019-11472.	imagemagick	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4821
1008	CVE-2019-15133	Medium	MEDIUM	In GIFLIB before 2019-02-16, a malformed GIF file triggers a divide-by-zero exception in the decoder function DGifSlurp in dgif_lib.c if the height field of the ImageSize data structure is equal to zero.	giflib	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4698
1009	CVE-2019-15132	Medium	MEDIUM	Zabbix through 4.4.0alpha1 allows User Enumeration. With login requests, it is possible to enumerate application usernames based on the variability of server responses (e.g., the Login name or password is incorrect and No permissions for system access messages, or just blocking for a number of seconds). This affects both api_jsonrpc.php and index.php.	zabbix	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1018-4695
1010	CVE-2019-15118	Medium	MEDIUM	check_input_term in sound/usb/mixer.c in the Linux kernel through 5.2.9 mishandles recursion, leading to kernel stack exhaustion.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4687
1011	CVE-2019-15117	Medium	HIGH	parse_audio_mixer_unit in sound/usb/mixer.c in the Linux kernel through 5.2.9 mishandles a short descriptor, leading to out-of-bounds memory access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	Not vulnerable	Not vulnerable	LIN1018-4688
1012	CVE-2019-15099	High	HIGH	drivers/net/wireless/ath/ath10k/usb.c in the Linux kernel through 5.2.8 has a NULL pointer dereference via an incomplete address in an endpoint descriptor.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.14	Not vulnerable	Not vulnerable	LIN1018-4689

	A	B	C	D	E	F	G	H	I	J	K	L	M
1013	CVE-2019-15098	High	HIGH	drivers/net/wireless/ath/ath6kl/usb.c in the Linux kernel through 5.2.8 has a NULL pointer dereference via an incomplete address in an endpoint descriptor.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4690
1014	CVE-2019-15090	Medium	HIGH	An issue was discovered in drivers/scsi/qedi/qedi_dbg.c in the Linux kernel before 5.1.12. In the qedi_dbg_* family of functions, there is an out-of-bounds read.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4691
1015	CVE-2019-15034	MEDIUM	HIGH	hw/display/bochs-display.c in QEMU 4.0.0 does not ensure a sufficient PCI config space allocation, leading to a buffer overflow involving the PCIe extended config space.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.15	Not vulnerable	10.20.12.0	LIN1019-4129
1016	CVE-2019-15031	LOW	HIGH	In the Linux kernel through 5.2.14 on the powerpc platform, a local user can read vector registers of other users' processes via an interrupt. To exploit the venerability, a local user starts a transaction (via the hardware transactional memory instruction tbegin) and then accesses vector registers. At some point, the vector registers will be corrupted with the values from a different local Linux process, because MSR_TM_ACTIVE is misused in arch/powerpc/kernel/process.c.	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4925
1017	CVE-2019-15030	LOW	HIGH	In the Linux kernel through 5.2.14 on the powerpc platform, a local user can read vector registers of other users' processes via a Facility Unavailable exception. To exploit the venerability, a local user starts a transaction (via the hardware transactional memory instruction tbegin) and then accesses vector registers. At some point, the vector registers will be corrupted with the values from a different local Linux process because of a missing arch/powerpc/kernel/process.c check.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4926
1018	CVE-2019-14981	MEDIUM	MEDIUM	In ImageMagick 7.x before 7.0.8-41 and 6.x before 6.9.10-41, there is a divide-by-zero vulnerability in the MeanShiftImage function. It allows an attacker to cause a denial of service by sending a crafted file.	imagemagick	Unchanged	Investigate	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4657
1019	CVE-2019-14980	MEDIUM	MEDIUM	In ImageMagick 7.x before 7.0.8-42 and 6.x before 6.9.10-42, there is a use after free vulnerability in the UnmapBlob function that allows an attacker to cause a denial of service by sending a crafted file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4658
1020	CVE-2019-14973	Medium	MEDIUM	_TIFFCheckMalloc and _TIFFCheckRealloc in tif_aux.c in LibTIFF through 4.0.10 mishandle Integer Overflow checks because they rely on compiler behavior that is undefined by the applicable C standards. This can, for example, lead to an application crash.	tiff	Unchanged	8.0.0.31	Investigate	10.17.41.20	10.18.44.10	10.19.45.1	Not vulnerable	LIN1018-4673
1021	CVE-2019-14970	MEDIUM	HIGH	A vulnerability in mkv::event_thread_t in VideoLAN VLC media player 3.0.7.1 allows remote attackers to trigger a heap-based buffer overflow via a crafted .mkv file.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4789
1022	CVE-2019-14907	MEDIUM	HIGH	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with log level = 3 (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).	samba	Unchanged	Not vulnerable	Not vulnerable	10.17.41.20	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3963
1023	CVE-2019-14902	MEDIUM	MEDIUM	There is an issue in all samba 4.11.x versions before 4.11.5, all samba 4.10.x versions before 4.10.12 and all samba 4.9.x versions before 4.9.18, where the removal of the right to create or modify a subtree would not automatically be taken away on all domain controllers.	samba	Unchanged	Not vulnerable	Not vulnerable	10.17.41.20	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3962
1024	CVE-2019-14901	HIGH	CRITICAL	A heap overflow flaw was found in the Linux kernel, all versions 3.x.x and 4.x.x before 4.18.0, in Marvell WiFi chip driver. The vulnerability allows a remote attacker to cause a system crash, resulting in a denial of service, or execute arbitrary code. The highest threat with this vulnerability is with the availability of the system. If code execution occurs, the code will run with the permissions of root. This will affect both confidentiality and integrity of files on the system.	linux	Unchanged	8.0.0.33	9.0.0.25	Investigate	10.18.44.15	10.19.45.5	Not vulnerable	LIN1019-3703
1025	CVE-2019-14897	HIGH	CRITICAL	A stack-based buffer overflow was found in the Linux kernel, version kernel-2.6.32, in Marvell WiFi chip driver. An attacker is able to cause a denial of service (system crash) or, possibly execute arbitrary code, when a STA works in IBSS mode (allows connecting stations together without the use of an AP) and connects to another STA.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.5	Not vulnerable	LIN1019-3704
1026	CVE-2019-14896	HIGH	CRITICAL	A vulnerability was found in marvell wifi chip driver in Linux kernel. There is a heap-based buffer overflow in lbs_ibss_join_existing function in drivers/net/wireless/marvell/libertas/cfg.c allows remote attackers to cause a denial of service(system crash) or possibly execute arbitrary code. When STA connects to AP, lbs_ibss_join_existing function will be called for STA.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.5	Not vulnerable	LIN1019-3665
1027	CVE-2019-14895	HIGH	CRITICAL	A heap-based buffer overflow was discovered in the Linux kernel, all versions 3.x.x and 4.x.x before 4.18.0, in Marvell WiFi chip driver. The flaw could occur when the station attempts a connection negotiation during the handling of the remote devices country settings. This could allow the remote device to cause a denial of service (system crash) or possibly execute arbitrary code.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.4	Not vulnerable	LIN1019-3705
1028	CVE-2019-14891	HIGH	CRITICAL	A flaw was found in cri-o, as a result of all pod-related processes being placed in the same memory cgroup. This can result in container management (conmon) processes being killed if a workload process triggers an out-of-memory (OOM) condition for the cgroup. An attacker could abuse this flaw to get host network access on an cri-o host.	cri-o	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	10.20.9.0	LIN1019-3668

	A	B	C	D	E	F	G	H	I	J	K	L	M
1029	CVE-2019-14889	HIGH	HIGH	A flaw was found with the libssh API function ssh_scp_new() in versions before 0.9.3 and before 0.8.8. When the libssh SCP client connects to a server, the scp command, which includes a user-provided path, is executed on the server-side. In case the library is used in a way where users can influence the third parameter of the function, it would become possible for an attacker to inject arbitrary commands, leading to a compromise of the remote target.	libssh2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3749
1030	CVE-2019-14870	MEDIUM	MEDIUM	All Samba versions 4.x.x before 4.9.17, 4.10.x before 4.10.11 and 4.11.x before 4.11.3 have an issue, where the S4U (MS-SFU) Kerberos delegation model includes a feature allowing for a subset of clients to be opted out of constrained delegation in any way, either S4U2Self or regular Kerberos authentication, by forcing all tickets for these clients to be non-forwardable. In AD this is implemented by a user attribute delegation_not_allowed (aka not-delegated), which translates to disallow-forwardable. However the Samba AD DC does not do that for S4U2Self and does set the forwardable flag even if the impersonated client has the not-delegated flag set.	samba	Unchanged	Investigate	Investigate	Investigate	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3746
1031	CVE-2019-14869	MEDIUM	HIGH	A flaw was found in all versions of ghostscript 9.x before 9.50, where the `.charkeys` procedure, where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. An attacker could abuse this flaw by creating a specially crafted PostScript file that could escalate privileges within the Ghostscript and access files outside of restricted areas or execute commands.	ghostscript	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.13	10.19.45.2	Not vulnerable	LIN1019-3475
1032	CVE-2019-14866	MEDIUM	HIGH	In all versions of cpio before 2.13 does not properly validate input files when generating TAR archives. When cpio is used to create TAR archives from paths an attacker can write to, the resulting archive may contain files with permissions the attacker did not have or in paths he did not have access to. Extracting those archives from a high-privilege user without carefully reviewing them may lead to the compromise of the system.	cpio	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-3897
1033	CVE-2019-14861	LOW	MEDIUM	All Samba versions 4.x.x before 4.9.17, 4.10.x before 4.10.11 and 4.11.x before 4.11.3 have an issue, where the (poorly named) dnsserver RPC pipe provides administrative facilities to modify DNS records and zones. Samba, when acting as an AD DC, stores DNS records in LDAP. In AD, the default permissions on the DNS partition allow creation of new records by authenticated users. This is used for example to allow machines to self-register in DNS. If a DNS record was created that case-insensitively matched the name of the zone, the ldb_qsort() and dns_name_compare() routines could be confused into reading memory prior to the list of DNS entries when responding to DnssrvEnumRecords() or DnssrvEnumRecords2() and so following invalid memory as a pointer.	samba	Unchanged	Investigate	Investigate	Investigate	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3747
1034	CVE-2019-14859	MEDIUM	CRITICAL	A flaw was found in all python-ecdsa versions before 0.13.3, where it did not correctly verify whether signatures used DER encoding. Without this verification, a malformed signature could be accepted, making the signature malleable. Without proper verification, an attacker could use a malleable signature to create false transactions.	python-ecdsa	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3901
1035	CVE-2019-14855	MEDIUM	HIGH	A flaw was found in the way certificate signatures could be forged using collisions found in the SHA-1 algorithm. An attacker could use this weakness to create forged certificate signatures. This issue affects GnuPG versions before 2.2.18.	gnupg	Unchanged	Investigate	9.0.0.25	10.17.41.20	10.18.44.16	10.19.45.6	Not vulnerable	LIN1019-4159
1036	CVE-2019-14847	MEDIUM	MEDIUM	A flaw was found in samba 4.0.0 before samba 4.9.15 and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue.	samba	Unchanged	Investigate	Investigate	10.17.41.19	10.18.44.12	10.19.45.2	Not vulnerable	LIN1019-3295
1037	CVE-2019-14842	HIGH	CRITICAL	Structured reply is a feature of the newstyle NBD protocol allowing the server to send a reply in chunks. A bounds check which was supposed to test for chunk offsets smaller than the beginning of the request did not work because of signed/unsigned confusion. If one of these chunks contains a negative offset then data under control of the server is written to memory before the read buffer supplied by the client. If the read buffer is located on the stack then this allows the stack return address from nbd_pread() to be trivially modified, allowing arbitrary code execution under the control of the server. If the buffer is located on the heap then other memory objects before the buffer can be overwritten, which again would usually lead to arbitrary code execution.	nbd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3667
1038	CVE-2019-14835	High	HIGH	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on the host.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4953
1039	CVE-2019-14834	MEDIUM	MEDIUM	A vulnerability was found in dnsmasq before version 2.81, where the memory leak allows remote attackers to cause a denial of service (memory consumption) via vectors involving DHCP response creation.	dnsmasq	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.4	10.20.9.0	LIN1019-3896

	A	B	C	D	E	F	G	H	I	J	K	L	M
1040	CVE-2019-14833	MEDIUM	MEDIUM	A flaw was found in Samba, all versions starting samba 4.5.0 before samba 4.9.15, samba 4.10.10, samba 4.11.2, in the way it handles a user password change or a new password for a samba user. The Samba Active Directory Domain Controller can be configured to use a custom script to check for password complexity. This configuration can fail to verify password complexity when non-ASCII characters are used in the password, which could lead to weak passwords being set for samba users, making it vulnerable to dictionary attacks.	samba	Unchanged	Investigate	Investigate	10.17.41.19	10.18.44.12	10.19.45.2	Not vulnerable	LIN1019-3296
1041	CVE-2019-14821	High	HIGH	An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hypervisor implements the Coalesced MMIO write operation. It operates on an MMIO ring buffer 'struct kvm_coalesced_mmio' object, wherein write indices 'ring->first' and 'ring->last' value could be supplied by a host user-space process. An unprivileged host user or process with access to '/dev/kvm' device could use this flaw to crash the host kernel, resulting in a denial of service or potentially escalating privileges on the system.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4954
1042	CVE-2019-14818	MEDIUM	HIGH	A flaw was found in all dpdk version 17.x.x before 17.11.8, 16.x.x before 16.11.10, 18.x.x before 18.11.4 and 19.x.x before 19.08.1 where a malicious master, or a container with access to vhost_user socket, can send specially crafted VRING_SET_NUM messages, resulting in a memory leak including file descriptors. This flaw could lead to a denial of service condition.	dpdk	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN1019-3468
1043	CVE-2019-14817	Medium	HIGH	A flaw was found in, ghostscript versions prior to 9.28, in the .pdfexectoken and other procedures where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.	ghostscript	Unchanged	Investigate	Investigate	10.17.41.20	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4832
1044	CVE-2019-14816	High	HIGH	There is heap-based buffer overflow in kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or possibly execute arbitrary code.	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4955
1045	CVE-2019-14815	HIGH	HIGH	kernel is vulnerable to a None	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1019-3604
1046	CVE-2019-14814	High	HIGH	There is heap-based buffer overflow in Linux kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or possibly execute arbitrary code.	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4956
1047	CVE-2019-14812	MEDIUM	HIGH	A flaw was found in all ghostscript versions 9.x before 9.50, in the .setuserparams2 procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3664
1048	CVE-2019-14811	Medium	HIGH	A flaw was found in, ghostscript versions prior to 9.28, in the .pdf_hook_DSC_Creator procedure where it did not properly secure its privileged calls, enabling scripts to bypass `-dSAFER` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.	ghostscript	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4833
1049	CVE-2019-14809	High	CRITICAL	net/url in Go before 1.11.13 and 1.12.x before 1.12.8 mishandles malformed hosts in URLs, leading to an authorization bypass in some applications. This is related to a Host field with a suffix appearing in neither Hostname() nor Port(), and is related to a non-numeric port number. For example, an attacker can compose a crafted javascript:// URL that results in a hostname of google.com.	go	Unchanged	Not vulnerable	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-4659
1050	CVE-2019-14778	MEDIUM	HIGH	The mkv::virtual_segment_c::seek method of demux/mkv/virtual_segment.cpp in VideoLAN VLC media player 3.0.7.1 has a use-after-free.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4790
1051	CVE-2019-14777	MEDIUM	HIGH	The Control function of demux/mkv/mkv.cpp in VideoLAN VLC media player 3.0.7.1 has a use-after-free.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4791
1052	CVE-2019-14776	MEDIUM	HIGH	A heap-based buffer over-read exists in DemuxInit() in demux/asf/asf.c in VideoLAN VLC media player 3.0.7.1 via a crafted .mkv file.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4792
1053	CVE-2019-14763	MEDIUM	MEDIUM	In the Linux kernel before 4.16.4, a double-locking error in drivers/usb/dwc3/gadget.c may potentially cause a deadlock with f_hid.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4639
1054	CVE-2019-14697	HIGH	CRITICAL	musl libc through 1.1.23 has an x87 floating-point stack adjustment imbalance, related to the math/i386/ directory. In some cases, use of this library could introduce out-of-bounds writes that are not present in an application's source code.	musl	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4654
1055	CVE-2019-14615	LOW	MEDIUM	Insufficient control flow in certain data structures for some Intel(R) Processors with Intel(R) Processor Graphics may allow an unauthenticated user to potentially enable information disclosure via local access.	linux	Updated	Investigate	Investigate	Investigate	Investigate	Investigate	Investigate	LIN1019-4267
1056	CVE-2019-14535	MEDIUM	HIGH	A divide-by-zero error exists in the SeekIndex function of demux/asf/asf.c in VideoLAN VLC media player 3.0.7.1. As a result, an FPE can be triggered via a crafted WMV file.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4793
1057	CVE-2019-14534	MEDIUM	MEDIUM	In VideoLAN VLC media player 3.0.7.1, there is a NULL pointer dereference at the function SeekPercent of demux/asf/asf.c that will lead to a denial of service attack.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4794
1058	CVE-2019-14533	MEDIUM	HIGH	The Control function of demux/asf/asf.c in VideoLAN VLC media player 3.0.7.1 has a use-after-free.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4795

	A	B	C	D	E	F	G	H	I	J	K	L	M
1059	CVE-2019-14513	Medium	HIGH	Improper bounds checking in Dnsmasq before 2.76 allows an attacker controlled DNS server to send large DNS packets that result in a read operation beyond the buffer allocated for the packet, a different vulnerability than CVE-2017-14491.	dnsmasq	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4616
1060	CVE-2019-14498	MEDIUM	HIGH	A divide-by-zero error exists in the Control function of demux/caf.c in VideoLAN VLC media player 3.0.7.1. As a result, an FPE can be triggered via a crafted CAF file.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4796
1061	CVE-2019-14494	Medium	MEDIUM	An issue was discovered in Poppler through 0.78.0. There is a divide-by-zero error in the function SplashOutputDev::tilingPatternFill at SplashOutputDev.cc.	poppler	Unchanged	Won't Fix	9.0.0.24	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4609
1062	CVE-2019-14493	Medium	HIGH	An issue was discovered in OpenCV before 4.1.1. There is a NULL pointer dereference in the function cv::XMLParser::parse at modules/core/src/persistence.cpp.	opencv	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4606
1063	CVE-2019-14492	Medium	HIGH	An issue was discovered in OpenCV before 3.4.7 and 4.x before 4.1.1. There is an out of bounds read/write in the function HaarEvaluator::OptFeature::calc in modules/objdetect/src/cascadedetect.hpp, which leads to denial of service.	opencv	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4607
1064	CVE-2019-14491	Medium	HIGH	An issue was discovered in OpenCV before 3.4.7 and 4.x before 4.1.1. There is an out of bounds read in the function cv::predictOrdered<cv::HaarEvaluator> in modules/objdetect/src/cascadedetect.hpp, which leads to denial of service.	opencv	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4608
1065	CVE-2019-14463	High	CRITICAL	An issue was discovered in libmodbus before 3.0.7 and 3.1.x before 3.1.5. There is an out-of-bounds read for the MODBUS_FC_WRITE_MULTIPLE_REGISTERS case, aka VD-1301.	libmodbus	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4662
1066	CVE-2019-14462	High	CRITICAL	An issue was discovered in libmodbus before 3.0.7 and 3.1.x before 3.1.5. There is an out-of-bounds read for the MODBUS_FC_WRITE_MULTIPLE_COILS case, aka VD-1302.	libmodbus	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4661
1067	CVE-2019-14444	MEDIUM	MEDIUM	apply_relocations in readelf.c in GNU Binutils 2.32 contains an integer overflow that allows attackers to trigger a write access violation (in byte_put_little_endian function in elfcomm.c) via an ELF file, as demonstrated by readelf.	binutils	Unchanged	8.0.0.31	9.0.0.23	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4569
1068	CVE-2019-14443	MEDIUM	MEDIUM	An issue was discovered in Libav 12.3. Division by zero in range_decode_culshift in libavcodec/apedec.c allows remote attackers to cause a denial of service (application crash), as demonstrated by avconv.	libav	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11282
1069	CVE-2019-14442	HIGH	MEDIUM	In mpc8_read_header in libavformat/mpc8.c in Libav 12.3, an input file can result in an avio_seek infinite loop and hang, with 100% CPU consumption. Attackers could leverage this vulnerability to cause a denial of service via a crafted file.	libav	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11283
1070	CVE-2019-14441	MEDIUM	MEDIUM	An issue was discovered in Libav 12.3. An access violation allows remote attackers to cause a denial of service (application crash), as demonstrated by avconv. This is related to ff_mpa_synth_filter_float in avcodec/mpegaudiodsp_template.c.	libav	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11284
1071	CVE-2019-14438	MEDIUM	HIGH	A heap-based buffer over-read in xiph_PackHeaders() in modules/demux/xiph.h in VideoLAN VLC media player 3.0.7.1 allows remote attackers to trigger a heap-based buffer over-read via a crafted .ogg file.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4797
1072	CVE-2019-14437	MEDIUM	HIGH	The xiph_SplitHeaders function in modules/demux/xiph.h in VideoLAN VLC media player 3.0.7.1 does not check array bounds properly. As a result, a heap-based buffer over-read can be triggered via a crafted .ogg file.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4798
1073	CVE-2019-14372	Medium	MEDIUM	In Libav 12.3, there is an infinite loop in the function wv_read_block_header() in the file wvdec.c.	libav	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11279
1074	CVE-2019-14371	Medium	MEDIUM	An issue was discovered in Libav 12.3. There is an infinite loop in the function mov_probe in the file libavformat/mov.c, related to offset and tag.	libav	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11280
1075	CVE-2019-14317	MEDIUM	MEDIUM	wolfSSL and wolfCrypt 4.1.0 and earlier (formerly known as CyaSSL) generate biased DSA nonces. This allows a remote attacker to compute the long term private key from several hundred DSA signatures via a lattice attack. The issue occurs because dsa.c fixes two bits of the generated nonces.	wolfssl	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3770
1076	CVE-2019-14287	HIGH	HIGH	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a sudo -u \#$((0xffffffff)) command.	sudo	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.1	Not vulnerable	LIN1018-5105
1077	CVE-2019-14284	LOW	MEDIUM	In the Linux kernel before 5.2.3, drivers/block/floppy.c allows a denial of service by setup_format_params division-by-zero. Two consecutive ioctls can trigger the bug: the first one should set the drive geometry with .sect and .rate values that make F_SECT_PER_TRACK be zero. Next, the floppy format operation should be called. It can be triggered by an unprivileged local user even when a floppy disk has not been inserted. NOTE: QEMU creates the floppy device by default.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4537
1078	CVE-2019-14283	MEDIUM	MEDIUM	In the Linux kernel before 5.2.3, set_geometry in drivers/block/floppy.c does not validate the sect and head fields, as demonstrated by an integer overflow and out-of-bounds read. It can be triggered by an unprivileged local user when a floppy disk has been inserted. NOTE: QEMU creates the floppy device by default.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4538
1079	CVE-2019-14274	MEDIUM	MEDIUM	MCPP 2.7.2 has a heap-based buffer overflow in the do_msg() function in support.c.	mcpp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4554
1080	CVE-2019-14271	HIGH	CRITICAL	In Docker 19.03.x before 19.03.1 linked against the GNU C Library (aka glibc), code injection can occur when the nsswitch facility dynamically loads a library inside a chroot that contains the contents of the container.	docker	Unchanged	Won't Fix	Investigate	Investigate	Investigate	10.19.45.1	Not vulnerable	LIN1018-4575

	A	B	C	D	E	F	G	H	I	J	K	L	M
1081	CVE-2019-14250	Medium	MEDIUM	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. simple_object_elf_match in simple-object-elf.c does not check for a zero shstrndx value, leading to an integer overflow and resultant heap-based buffer overflow.	binutils	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4484
1082	CVE-2019-14248	MEDIUM	MEDIUM	In libnasm.a in Netwide Assembler (NASM) 2.14.xx, asm/pragma.c allows a NULL pointer dereference in process_pragma, search_pragma_list, and nasm_set_limit when %pragma limit is mishandled.	nasm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.2	10.20.3.0	LIN1018-4485
1083	CVE-2019-14204	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_umountall_reply.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4578
1084	CVE-2019-14203	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_mount_reply.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4579
1085	CVE-2019-14202	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_readlink_reply.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4580
1086	CVE-2019-14201	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_lookup_reply.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4581
1087	CVE-2019-14200	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: rpc_lookup_reply.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4582
1088	CVE-2019-14199	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy when parsing a UDP packet due to a net_process_received_packet integer underflow during an *udp_packet_handler call.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4583
1089	CVE-2019-14198	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_read_reply when calling store_block in the NFSv3 case.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4584
1090	CVE-2019-14197	Medium	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is a read of out-of-bounds data at nfs_read_reply.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4585
1091	CVE-2019-14196	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_lookup_reply.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4586
1092	CVE-2019-14195	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with unvalidated length at nfs_readlink_reply in the else block after calculating the new path length.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4587
1093	CVE-2019-14194	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_read_reply when calling store_block in the NFSv2 case.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4588
1094	CVE-2019-14193	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with an unvalidated length at nfs_readlink_reply, in the if block after calculating the new path length.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4589
1095	CVE-2019-14192	High	CRITICAL	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy when parsing a UDP packet due to a net_process_received_packet integer underflow during an nc_input_packet call.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4590
1096	CVE-2019-13962	High	CRITICAL	lavc_CopyPicture in modules/codec/avcodec/video.c in VideoLAN VLC media player through 3.0.7 has a heap-based buffer over-read because it does not properly validate the width and height.	vlc	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4462
1097	CVE-2019-13960	MEDIUM	MEDIUM	** DISPUTED ** In libjpeg-turbo 2.0.2, a large amount of memory can be used during processing of an invalid progressive JPEG image containing incorrect width and height values in the image header. NOTE: the vendor's expectation, for use cases in which this memory usage would be a denial of service, is that the application should interpret libjpeg warnings as fatal errors (aborting decompression) and/or set limits on resource consumption or image sizes.	libjpeg-turbo	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1019-1858
1098	CVE-2019-1387	MEDIUM	HIGH	An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. Recursive clones are currently affected by a vulnerability that is caused by too-lax validation of submodule names, allowing very targeted attacks via remote code execution in recursive clones.	git	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	10.19.45.6	Not vulnerable	LIN1019-3768
1099	CVE-2019-13648	Medium	MEDIUM	In the Linux kernel through 5.2.1 on the powerpc platform, when hardware transactional memory is disabled, a local user can cause a denial of service (TM Bad Thing exception and system crash) via a sigreturn() system call that sends a crafted signal frame. This affects arch/powerpc/kernel/signal_32.c and arch/powerpc/kernel/signal_64.c.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.18	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4461
1100	CVE-2019-13638	HIGH	HIGH	GNU patch through 2.7.6 is vulnerable to OS shell command injection that can be exploited by opening a crafted patch file that contains an ed style diff payload with shell metacharacters. The ed editor does not need to be present on the vulnerable system. This is different from CVE-2018-1000156.	patch	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	10.19.45.1	Not vulnerable	LIN1018-4539
1101	CVE-2019-13636	Medium	MEDIUM	In GNU patch through 2.7.6, the following of symlinks is mishandled in certain cases other than input files. This affects inp.c and util.c.	patch	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4457
1102	CVE-2019-13631	Medium	MEDIUM	In parse_hid_report_descriptor in drivers/input/tablet/gtco.c in the Linux kernel through 5.2.1, a malicious USB device can send an HID report that triggers an out-of-bounds write during generation of debugging messages.	linux	Unchanged	Investigate	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4458

	A	B	C	D	E	F	G	H	I	J	K	L	M
1103	CVE-2019-13628	Low	MEDIUM	wolfSSL and wolfCrypt 4.0.0 and earlier (when configured without --enable-fpecc, --enable-sp, or --enable-sp-math) contain a timing side channel in ECDSA signature generation. This allows a local attacker, able to precisely measure the duration of signature operations, to infer information about the nonces used and potentially mount a lattice attack to recover the private key used. The issue occurs because ecc.c scalar multiplication might leak the bit length.	wolfssl	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5012
1104	CVE-2019-13627	Medium	HIGH	It was discovered that there was a ECDSA timing attack in the libgcrypt20 cryptographic library. Version affected: 1.8.4-5, 1.7.6-2+deb9u3, and 1.6.3-2+deb8u4. Versions fixed: 1.8.5-2 and 1.6.3-2+deb8u7.	libgcrypt	Updated	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	10.19.45.6	10.20.15.0	LIN1018-5046
1105	CVE-2019-13626	Medium	MEDIUM	SDL (Simple DirectMedia Layer) 2.x through 2.0.9 has a heap-based buffer over-read in Fill_IMA_ADPCM_block, caused by an integer overflow in IMA_ADPCM_decode() in audio/SDL_wave.c.	libsdl	Unchanged	Investigate	Investigate	Investigate	Investigate	10.19.45.1	Not vulnerable	LIN1018-4452
1106	CVE-2019-13619	Medium	HIGH	In Wireshark 3.0.0 to 3.0.2, 2.6.0 to 2.6.9, and 2.4.0 to 2.4.15, the ASN.1 BER dissector and related dissectors could crash. This was addressed in epan/asn1.c by properly restricting buffer increments.	wireshark	Unchanged	Not vulnerable	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4459
1107	CVE-2019-13617	Medium	MEDIUM	njs through 0.3.3, used in NGINX, has a heap-based buffer over-read in nxt_vsprintf in nxt/nxt_sprintf.c during error handling, as demonstrated by an njs_regexp_literal call that leads to an njs_parser_lexer_error call and then an njs_parser_scope_error call.	nginx	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4447
1108	CVE-2019-13616	Medium	HIGH	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in BlitNtoN in video/SDL_blit_N.c when called from SDL_SoftBlit in video/SDL_blit.c.	libsdl	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	10.19.45.1	Not vulnerable	LIN1018-4448
1109	CVE-2019-13615	Medium	MEDIUM	libebml before 1.3.6, as used in the MKV module in VideoLAN VLC Media Player binaries before 3.0.3, has a heap-based buffer over-read in EbmlElement::FindNextElement.	libebml	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4449
1110	CVE-2019-13602	Medium	HIGH	An Integer Underflow in MP4_EIA608_Convert() in modules/demux/mp4/mp4.c in VideoLAN VLC media player through 3.0.7.1 allows remote attackers to cause a denial of service (heap-based buffer overflow and crash) or possibly have unspecified other impact via a crafted .mp4 file.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4441
1111	CVE-2019-13590	MEDIUM	HIGH	An issue was discovered in libsox.a in SoX 14.4.2. In sox-fmt.h (startread function), there is an integer overflow on the result of integer addition (wraparound to 0) fed into the lsx_calloc macro that wraps malloc. When a NULL pointer is returned, it is used without a prior check that it is a valid pointer, leading to a NULL pointer dereference on lsx_readbuf in formats_i.c.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4431
1112	CVE-2019-13565	MEDIUM	HIGH	An issue was discovered in OpenLDAP 2.x before 2.4.48. When using SASL authentication and session encryption, and relying on the SASL security layers in slapd access controls, it is possible to obtain access that would otherwise be denied via a simple bind for any identity covered in those ACLs. After the first SASL bind is completed, the sasl_ssf value is retained for all new non-SASL connections. Depending on the ACL configuration, this can affect different types of operations (searches, modifications, etc.). In other words, a successful authorization step completed by one user affects the authorization requirement for a different user.	openldap	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4540
1113	CVE-2019-1348	LOW	LOW	An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. The --export-marks option of git fast-import is exposed also via the in-stream command feature export-marks=... and it allows overwriting arbitrary paths.	git	Unchanged	Investigate	Investigate	Investigate	Investigate	10.19.45.6	Not vulnerable	LIN1019-3760
1114	CVE-2019-13456	LOW	MEDIUM	In FreeRADIUS 3.0 through 3.0.19, on average 1 in every 2048 EAP-pwd handshakes fails because the password element cannot be found within 10 iterations of the hunting and pecking loop. This leaks information that an attacker can use to recover the password of any user. This information leakage is similar to the Dragonblood attack and CVE-2019-9494.	freeradius	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	Not vulnerable	LIN1019-3753
1115	CVE-2019-13454	Medium	MEDIUM	ImageMagick 7.0.8-54 Q16 allows Division by Zero in RemoveDuplicateLayers in MagickCore/layer.c.	imagemagick	Unchanged	Investigate	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4417
1116	CVE-2019-13391	Medium	HIGH	In ImageMagick 7.0.8-50 Q16, ComplexImages in MagickCore/fourier.c has a heap-based buffer over-read because of incorrect calls to GetCacheViewVirtualPixels.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4416
1117	CVE-2019-13390	Medium	MEDIUM	In FFmpeg 4.1.3, there is a division by zero at adx_write_trailer in libavformat/rawenc.c. This may be related to two NULL pointers passed as arguments at libavcodec/frame_thread_encoder.c.	ffmpeg	Unchanged	Won't Fix	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4415
1118	CVE-2019-13377	Medium	MEDIUM	The implementations of SAE and EAP-pwd in hostapd and wpa_supplicant 2.x through 2.8 are vulnerable to side-channel attacks as a result of observable timing differences and cache access patterns when Brainpool curves are used. An attacker may be able to gain leaked information from a side-channel attack that can be used for full password recovery.	hostapd&wpa-supplicant	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4701
1119	CVE-2019-13345	Medium	MEDIUM	The cachemgr.cgi web module of Squid through 4.7 has XSS via the user_name or auth parameter.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4445
1120	CVE-2019-13312	Medium	HIGH	block_cmp() in libavcodec/zmbvenc.c in FFmpeg 4.1.3 has a heap-based buffer over-read.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4413
1121	CVE-2019-13311	Medium	MEDIUM	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of a wand/mogrify.c error.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4394
1122	CVE-2019-13310	Medium	MEDIUM	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of an error in MagickWand/mogrify.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4395

	A	B	C	D	E	F	G	H	I	J	K	L	M
1123	CVE-2019-13309	Medium	MEDIUM	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of mishandling the NoSuchImage error in CLIListOperatorImages in MagickWand/operation.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4396
1124	CVE-2019-13308	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow in MagickCore/fourier.c in ComplexImage.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4397
1125	CVE-2019-13307	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling rows.	imagemagick	Unchanged	Investigate	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4398
1126	CVE-2019-13306	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of off-by-one errors.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4399
1127	CVE-2019-13305	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced strncpy and an off-by-one error.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4400
1128	CVE-2019-13304	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced assignment.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4401
1129	CVE-2019-13303	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read in MagickCore/composite.c in CompositeImage.	imagemagick	Unchanged	Not vulnerable	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4402
1130	CVE-2019-13302	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read in MagickCore/fourier.c in ComplexImages.	imagemagick	Unchanged	Not vulnerable	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4403
1131	CVE-2019-13301	Medium	MEDIUM	ImageMagick 7.0.8-50 Q16 has memory leaks in AcquireMagickMemory because of an AnnotateImage error.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4404
1132	CVE-2019-13300	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling columns.	imagemagick	Unchanged	Investigate	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4405
1133	CVE-2019-13299	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/pixel-accessor.h in GetPixelChannel.	imagemagick	Unchanged	Not vulnerable	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4406
1134	CVE-2019-13298	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/pixel-accessor.h in SetPixelViaPixelInfo because of a MagickCore/enhance.c error.	imagemagick	Unchanged	Not vulnerable	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4407
1135	CVE-2019-13297	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a height of zero is mishandled.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4408
1136	CVE-2019-13296	Medium	MEDIUM	ImageMagick 7.0.8-50 Q16 has direct memory leaks in AcquireMagickMemory because of an error in CLIListOperatorImages in MagickWand/operation.c for a NULL value.	imagemagick	Unchanged	Not vulnerable	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4409
1137	CVE-2019-13295	Medium	HIGH	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a width of zero is mishandled.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4410
1138	CVE-2019-13272	High	HIGH	In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments.	linux	Unchanged	Not vulnerable	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4450
1139	CVE-2019-13233	Medium	HIGH	In arch/x86/lib/insn-eval.c in the Linux kernel before 5.1.9, there is a use-after-free for access to an LDT entry because of a race condition between modify_ldt() and a #BR exception for an MPX bounds violation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4389
1140	CVE-2019-13232	Medium	HIGH	Info-ZIP UnZip 6.0 mishandles the overlapping of files inside a ZIP container, leading to denial of service (resource consumption), aka a better zip bomb issue.	unzip	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4392
1141	CVE-2019-13164	Medium	HIGH	qemu-bridge-helper.c in QEMU 4.0.0 does not ensure that a network interface name (obtained from bridge.conf or a --br=bridge option) is limited to the IFNAMSIZ size, which can lead to an ACL bypass.	qemu	Unchanged	8.0.0.31	9.0.0.23	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4383
1142	CVE-2019-13147	Medium	MEDIUM	In Audio File Library (aka audiofile) 0.3.6, there exists one NULL pointer dereference bug in ulaw2linear_buf in G711.cpp in libmodules.a that allows an attacker to cause a denial of service via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4381
1143	CVE-2019-13139	MEDIUM	HIGH	In Docker before 18.09.4, an attacker who is capable of supplying or manipulating the build path for the docker build command would be able to gain command execution. An issue exists in the way docker build processes remote git URLs, and results in command injection into the underlying git clone command, leading to code execution in the context of the user executing the docker build command. This occurs because git ref can be misinterpreted as a flag.	docker	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-4753
1144	CVE-2019-13137	Medium	MEDIUM	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadPSImage in coders/ps.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4374
1145	CVE-2019-13136	Medium	HIGH	ImageMagick before 7.0.8-50 has an integer overflow vulnerability in the function TIFFSeekCustomStream in coders/tiff.c.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4375
1146	CVE-2019-13135	Medium	HIGH	ImageMagick before 7.0.8-50 has a use of uninitialized value vulnerability in the function ReadCUTImage in coders/cut.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4376
1147	CVE-2019-13134	Medium	MEDIUM	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadVIFFImage in coders/viff.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4377
1148	CVE-2019-13133	Medium	MEDIUM	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadBMPImage in coders/bmp.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4378

	A	B	C	D	E	F	G	H	I	J	K	L	M
1149	CVE-2019-13132	HIGH	CRITICAL	In ZeroMQ libzmq before 4.0.9, 4.1.x before 4.1.7, and 4.2.x before 4.3.2, a remote, unauthenticated client connecting to a libzmq application, running with a socket listening with CURVE encryption/authentication enabled, may cause a stack overflow and overwrite the stack with arbitrary data, due to a buffer overflow in the library. Users running public servers with the above configuration are highly encouraged to upgrade as soon as possible, as there are no known mitigations.	zeromq	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4442
1150	CVE-2019-13118	Medium	HIGH	In numbers.c in libxslt 1.1.33, a type holding grouping characters of an xsl:number instruction was too narrow and an invalid character/length combination could be passed to xsltNumberFormatDecimal, leading to a read of uninitialized stack data.	libxslt	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4379
1151	CVE-2019-13117	Medium	HIGH	In numbers.c in libxslt 1.1.33, an xsl:number with certain format strings could lead to a uninitialized read in xsltNumberFormatInsertNumbers. This could allow an attacker to discern whether a byte on the stack contains the characters A, a, I, i, or 0, or any other character.	libxslt	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4380
1152	CVE-2019-13115	Medium	HIGH	In libssh2 before 1.9.0, kex_method_diffie_hellman_group_exchange_sha256_key_exchange in kex.c has an integer overflow that could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. This is related to an _libssh2_check_length mistake, and is different from the various issues fixed in 1.8.1, such as CVE-2019-3855.	libssh2	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4451
1153	CVE-2019-13106	HIGH	HIGH	Das U-Boot versions 2016.09 through 2019.07-rc4 can memset() too much data while reading a crafted ext4 filesystem, which results in a stack buffer overflow and likely code execution.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4631
1154	CVE-2019-13105	MEDIUM	HIGH	Das U-Boot versions 2019.07-rc1 through 2019.07-rc4 can double-free a cached block of data when listing files in a crafted ext4 filesystem.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4630
1155	CVE-2019-13104	MEDIUM	HIGH	In Das U-Boot versions 2016.11-rc1 through 2019.07-rc4, an underflow can cause memcpy() to overwrite a very large amount of data (including the whole stack) while reading a crafted ext4 filesystem.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4624
1156	CVE-2019-13103	MEDIUM	CRITICAL	A crafted self-referential DOS partition table will cause all Das U-Boot versions through 2019.07-rc4 to infinitely recurse, causing the stack to grow infinitely and eventually either crash or overwrite other data.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4576
1157	CVE-2019-13067	HIGH	CRITICAL	njs through 0.3.3, used in NGINX, has a buffer over-read in nxt_utf8_decode in nxt/nxt_utf8.c. This issue occurs after the fix for CVE-2019-12207 is in place.	nginx	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4369
1158	CVE-2019-13057	LOW	MEDIUM	An issue was discovered in the server in OpenLDAP before 2.4.48. When the server administrator delegates rootDN (database admin) privileges for certain databases but wants to maintain isolation (e.g., for multi-tenant deployments), slapd does not properly stop a rootDN from requesting authorization as an identity from another database during a SASL bind or with a proxyAuthz (RFC 4370) control. (It is not a common configuration to deploy a system where the server administrator and a DB administrator enjoy different levels of trust.)	openldap	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4541
1159	CVE-2019-13050	MEDIUM	HIGH	Interaction between the sks-keyserver code through 1.2.0 of the SKS keyserver network, and GnuPG through 2.2.16, makes it risky to have a GnuPG keyserver configuration line referring to a host on the SKS keyserver network. Retrieving data from this network may cause a persistent denial of service, because of a Certificate Spamming Attack.	gnupg	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-4370
1160	CVE-2019-13045	MEDIUM	HIGH	Irssi before 1.0.8, 1.1.x before 1.1.3, and 1.2.x before 1.2.1, when SASL is enabled, has a use after free when sending SASL login to the server.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4371
1161	CVE-2019-13012	MEDIUM	HIGH	The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.59.1 creates directories using g_file_make_directory_with_parents (kfsb->dir, NULL, NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used; for files, default file permissions are used. This is similar to CVE-2019-12450.	glib-2.0	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4368
1162	CVE-2019-12984	Medium	MEDIUM	A NULL pointer dereference vulnerability in the function nfc_genl_deactivate_target() in net/nfc/netlink.c in the Linux kernel before 5.1.13 can be triggered by a malicious user-mode program that omits certain NFC attributes, leading to denial of service.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4362
1163	CVE-2019-12979	Medium	HIGH	ImageMagick 7.0.8-34 has a use of uninitialized value vulnerability in the SyncImageSettings function in MagickCore/image.c. This is related to AcquireImage in magick/image.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4356
1164	CVE-2019-12978	Medium	HIGH	ImageMagick 7.0.8-34 has a use of uninitialized value vulnerability in the ReadPANGOImage function in coders/pango.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4355
1165	CVE-2019-12977	Medium	HIGH	ImageMagick 7.0.8-34 has a use of uninitialized value vulnerability in the WriteJP2Image function in coders/jp2.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4354
1166	CVE-2019-12976	Medium	MEDIUM	ImageMagick 7.0.8-34 has a memory leak in the ReadPCLImage function in coders/pcl.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4353
1167	CVE-2019-12975	Medium	MEDIUM	ImageMagick 7.0.8-34 has a memory leak vulnerability in the WriteDPXImage function in coders/dpx.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4352

	A	B	C	D	E	F	G	H	I	J	K	L	M
1168	CVE-2019-12974	Medium	MEDIUM	A NULL pointer dereference in the function ReadPANGOImage in coders/pango.c and the function ReadVIDImage in coders/vid.c in ImageMagick 7.0.8-34 allows remote attackers to cause a denial of service via a crafted image.	imagemagick	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4361
1169	CVE-2019-12973	Medium	MEDIUM	In OpenJPEG 2.3.1, there is excessive iteration in the opj_t1_encode_cblks function of openjp2/t1.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file. This issue is similar to CVE-2018-6616.	openjpeg	Unchanged	Won't Fix	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4360
1170	CVE-2019-12972	Medium	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. There is a heap-based buffer over-read in _bfd_dopmt in bfd.c because elf_object_p in elfcode.h mishandles an e_shstrndx section of type SHT_GROUP by omitting a trailing '\0' character.	binutils	Unchanged	8.0.0.31	9.0.0.23	10.17.41.18	10.18.44.11	10.19.45.1	Not vulnerable	LIN1018-4347
1171	CVE-2019-12929	High	CRITICAL	The QMP guest_exec command in QEMU 4.0.0 and earlier is prone to OS command injection, which allows the attacker to achieve code execution, denial of service, or information disclosure by sending a crafted QMP command to the listening server.	qemu	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-4340
1172	CVE-2019-12928	High	CRITICAL	The QMP migrate command in QEMU version 4.0.0 and earlier is vulnerable to OS command injection, which allows the remote attacker to achieve code execution, denial of service, or information disclosure by sending a crafted QMP command to the listening server.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4339
1173	CVE-2019-12922	Medium	MEDIUM	A CSRF issue in phpMyAdmin 4.9.0.1 allows deletion of any server in the Setup page.	phpmyadmin	Unchanged	Vulnerable	Vulnerable	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4932
1174	CVE-2019-12904	Medium	MEDIUM	In Libgcrypt 1.8.4, the C implementation of AES is vulnerable to a flush-and-reload side-channel attack because physical addresses are available to other processes. (The C implementation is used on platforms where an assembly-language implementation is unavailable.)	libgcrypt	Unchanged	Investigate	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4317
1175	CVE-2019-12900	High	CRITICAL	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.	bzip2	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	10.19.45.6	Not vulnerable	LIN1018-4316
1176	CVE-2019-12881	Medium	HIGH	i915_gem_userptr_get_pages in drivers/gpu/drm/i915/i915_gem_userptr.c in the Linux kernel 4.15.0 on Ubuntu 18.04.2 allows local users to cause a denial of service (NULL pointer dereference and BUG) or possibly have unspecified other impact via crafted ioctl calls to /dev/dri/card0.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4304
1177	CVE-2019-12874	High	CRITICAL	An issue was discovered in zlib_decompress_extra in modules/demux/mkv/util.cpp in VideoLAN VLC media player 3.x through 3.0.7. The Matroska demuxer, while parsing a malformed MKV file type, has a double free.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4305
1178	CVE-2019-12840	High	HIGH	In Webmin through 1.910, any user authorized to the Package Updates module can execute arbitrary commands with root privileges via the data parameter to update.cgi.	webmin	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4283
1179	CVE-2019-12819	Low	MEDIUM	An issue was discovered in the Linux kernel before 5.0. The function __mdiobus_register() in drivers/net/phy/mdio_bus.c calls put_device(), which will trigger a fixed_mdio_bus_init use-after-free. This will cause a denial of service.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4284
1180	CVE-2019-12818	Medium	HIGH	An issue was discovered in the Linux kernel before 4.20.15. The nfc_llcp_build_tlv function in net/nfc/llcp_commands.c may return NULL. If the caller does not check for this, it will trigger a NULL pointer dereference. This will cause denial of service. This affects nfc_llcp_build_gb in net/nfc/llcp_core.c.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4285
1181	CVE-2019-12817	Medium	HIGH	arch/powerpc/mm/ mmu_context_book3s64.c in the Linux kernel before 5.1.15 for powerpc has a bug where unrelated processes may be able to read/write to one another's virtual memory under certain conditions via an mmap above 512 TB. Only a subset of powerpc systems are affected.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4343
1182	CVE-2019-12816	Medium	HIGH	Modules.cpp in ZNC before 1.7.4-rc1 allows remote authenticated non-admin users to escalate privileges and execute arbitrary code by loading a module with a crafted name.	znc	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4286
1183	CVE-2019-12815	High	CRITICAL	An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306.	proftpd	Unchanged	8.0.0.31	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4557
1184	CVE-2019-12795	Medium	HIGH	daemon/gvfsdaemon.c in gvfsd from GNOME gvfs before 1.38.3, 1.40.x before 1.40.2, and 1.41.x before 1.41.3 opened a private D-Bus server socket without configuring an authorization rule. A local attacker could connect to this server socket and issue D-Bus method calls. (Note that the server socket only accepts a single connection, so the attacker would have to discover the server and connect to the socket before its owner does.)	gvfs	Unchanged	Won't Fix	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4266
1185	CVE-2019-12779	Medium	HIGH	libqb before 1.0.5 allows local users to overwrite arbitrary files via a symlink attack, because it uses predictable filenames (under /dev/shm and /tmp) without O_EXCL.	libqb	Unchanged	Won't Fix	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4252

	A	B	C	D	E	F	G	H	I	J	K	L	M
1186	CVE-2019-12749	Low	HIGH	dbus before 1.10.28, 1.12.x before 1.12.16, and 1.13.x before 1.13.12, as used in DBusServer in Canonical Upstart in Ubuntu 14.04 (and in some, less common, uses of dbus-daemon), allows cookie spoofing because of symlink mishandling in the reference implementation of DBUS_COOKIE_SHA1 in the libdbus library. (This only affects the DBUS_COOKIE_SHA1 authentication mechanism.) A malicious client with write access to its own home directory could manipulate a ~/.dbus-keyrings symlink to cause a DBusServer with a different uid to read and write in unintended locations. In the worst case, this could result in the DBusServer reusing a cookie that is known to the malicious client, and treating that cookie as evidence that a subsequent client connection came from an attacker-chosen uid, allowing authentication bypass.	dbus	Unchanged	8.0.0.31	9.0.0.22	Vulnerable	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4265
1187	CVE-2019-12735	High	HIGH	getchar.c in Vim before 8.1.1365 and Neovim before 0.3.6 allows remote attackers to execute arbitrary OS commands via the :source! command in a modeline, as demonstrated by execute in Vim, and assert_fails or nvim_input in Neovim.	vim	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4242
1188	CVE-2019-12730	High	CRITICAL	aa_read_header in libavformat/aadec.c in FFmpeg before 3.2.14 does not check for sscanf failure and consequently allows use of uninitialized variables.	ffmpeg	Unchanged	Won't Fix	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4253
1189	CVE-2019-12625	MEDIUM	HIGH	ClamAV versions prior to 0.101.3 are susceptible to a zip bomb vulnerability where an unauthenticated attacker can cause a denial of service condition by sending crafted messages to an affected system.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Investigate	LIN1019-3298
1190	CVE-2019-12616	Medium	MEDIUM	An issue was discovered in phpMyAdmin before 4.9.0. A vulnerability was found that allows an attacker to trigger a CSRF attack against a phpMyAdmin user. The attacker can trick the user, for instance through a broken <img> tag pointing at the victim's phpMyAdmin database, and the attacker can potentially deliver a payload (such as a specific INSERT or DELETE statement) to the victim.	phpmyadmin	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4243
1191	CVE-2019-12615	High	HIGH	An issue was discovered in get_vdev_port_node_info in arch/sparc/kernel/mdesc.c in the Linux kernel through 5.1.6. There is an unchecked kstrdup_const of node_info->vdev_port.name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4245
1192	CVE-2019-12614	High	HIGH	An issue was discovered in dlpar_parse_cc_property in arch/powerpc/platforms/pseries/dlpar.c in the Linux kernel through 5.1.6. There is an unchecked kstrdup of prop->name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4246
1193	CVE-2019-12585	High	CRITICAL	Apcupsd 0.3.91_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an Arbitrary Command Execution issue in apcupsd_status.php.	apcupsd	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-8644
1194	CVE-2019-12584	Medium	MEDIUM	Apcupsd 0.3.91_5, as used in pfSense through 2.4.4-RELEASE-p3 and other products, has an XSS issue in apcupsd_status.php.	apcupsd	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-8643
1195	CVE-2019-12529	MEDIUM	MEDIUM	An issue was discovered in Squid 2.x through 2.7.STABLE9, 3.x through 3.5.28, and 4.x through 4.7. When Squid is configured to use Basic Authentication, the Proxy-Authorization header is parsed via uudecode. uudecode determines how many bytes will be decoded by iterating over the input and checking its table. The length is then used to start decoding the string. There are no checks to ensure that the length it calculates isn't greater than the input buffer. This leads to adjacent memory being decoded as well. An attacker would not be able to retrieve the decoded data unless the Squid maintainer had configured the display of usernames on error pages.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4428
1196	CVE-2019-12528	MEDIUM	HIGH	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	squid	Unchanged	8.0.0.33	9.0.0.25	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4005
1197	CVE-2019-12527	MEDIUM	HIGH	An issue was discovered in Squid 4.0.23 through 4.7. When checking Basic Authentication with HttpHeader::getAuth, Squid uses a global buffer to store the decoded data. Squid does not check that the decoded length isn't greater than the buffer, leading to a heap-based buffer overflow with user controlled data.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4429
1198	CVE-2019-12526	HIGH	CRITICAL	An issue was discovered in Squid before 4.9. URN response handling in Squid suffers from a heap-based buffer overflow. When receiving data from a remote server in response to an URN request, Squid fails to ensure that the response can fit within the buffer. This leads to attacker controlled data overflowing in the heap.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3658
1199	CVE-2019-12525	HIGH	CRITICAL	An issue was discovered in Squid 3.3.9 through 3.5.28 and 4.x through 4.7. When Squid is configured to use Digest authentication, it parses the header Proxy-Authorization. It searches for certain tokens such as domain, uri, and qop. Squid checks if this token's value starts with a quote and ends with one. If so, it performs a memcpy of its length minus 2. Squid never checks whether the value is just a single quote (which would satisfy its requirements), leading to a memcpy of its length minus 1.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4430
1200	CVE-2019-12523	MEDIUM	CRITICAL	An issue was discovered in Squid before 4.9. When handling a URN request, a corresponding HTTP request is made. This HTTP request doesn't go through the access checks that incoming HTTP requests go through. This causes all access checks to be bypassed and allows access to restricted HTTP servers, e.g., an attacker can connect to HTTP servers that only listen on localhost.	squid	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3659

	A	B	C	D	E	F	G	H	I	J	K	L	M
1201	CVE-2019-12456	High	HIGH	An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3sas/mpt3sas_ctl.c in the Linux kernel through 5.1.5. It allows local users to cause a denial of service or possibly have unspecified other impact by changing the value of ioc_number between two kernel reads of that value, aka a double fetch vulnerability.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	10.19.45.1	10.20.3.0	LIN1018-4279
1202	CVE-2019-12455	Medium	MEDIUM	An issue was discovered in sunxi_divs_clk_setup in drivers/clk/sunxi/clk-sunxi.c in the Linux kernel through 5.1.5. There is an unchecked kstrndup of derived_name, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.18	10.18.44.11	10.19.45.1	10.20.3.0	LIN1018-4183
1203	CVE-2019-12454	High	HIGH	An issue was discovered in wcd9335_codec_enable_dec in sound/soc/codecs/wcd9335.c in the Linux kernel through 5.1.5. It uses kstrndup instead of kmemdup_nul, which allows attackers to have an unspecified impact via unknown vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.1	10.20.3.0	LIN1018-4184
1204	CVE-2019-12450	High	CRITICAL	file_copy_fallback in gio/gfile.c in GNOME GLib 2.15.0 through 2.61.1 does not properly restrict file permissions while a copy operation is in progress. Instead, default permissions are used.	glib-2.0	Unchanged	8.0.0.31	Investigate	10.17.41.17	10.18.44.8	10.19.45.1	Not vulnerable	LIN1018-4188
1205	CVE-2019-12449	High	CRITICAL	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c mishandles a file's user and group ownership during move (and copy with G_FILE_COPY_ALL_METADATA) operations from admin:// to file:// URIs, because root privileges are unavailable.	gvfs	Unchanged	Not vulnerable	Not vulnerable	10.17.41.17	10.18.44.8	10.19.45.1	Not vulnerable	LIN1018-4185
1206	CVE-2019-12448	Medium	HIGH	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c has race conditions because the admin backend doesn't implement query_info_on_read/write.	gvfs	Unchanged	Not vulnerable	Not vulnerable	10.17.41.17	10.18.44.8	10.19.45.1	Not vulnerable	LIN1018-4186
1207	CVE-2019-12447	High	CRITICAL	An issue was discovered in GNOME gvfs 1.29.4 through 1.41.2. daemon/gvfsbackendadmin.c mishandles file ownership because setfsuid is not used.	gvfs	Unchanged	Not vulnerable	Not vulnerable	10.17.41.17	10.18.44.8	10.19.45.1	Not vulnerable	LIN1018-4187
1208	CVE-2019-12436	Medium	MEDIUM	Samba 4.10.x before 4.10.5 has a NULL pointer dereference, leading to an AD DC LDAP server Denial of Service. This is related to an attacker using the paged search control. The attacker must have directory read access in order to attempt an exploit.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4299
1209	CVE-2019-12435	Medium	MEDIUM	Samba 4.9.x before 4.9.9 and 4.10.x before 4.10.5 has a NULL pointer dereference, leading to Denial of Service. This is related to the AD DC DNS management server (dnsserver) RPC server process.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4298
1210	CVE-2019-12382	Medium	MEDIUM	An issue was discovered in drm_load_edid_firmware in drivers/gpu/drm/drm_edid_load.c in the Linux kernel through 5.1.5. There is an unchecked kstrdup of fwstr, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	linux	Unchanged	Not vulnerable	9.0.0.24	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4166
1211	CVE-2019-12381	Medium	MEDIUM	An issue was discovered in ip_ra_control in net/ipv4/ip_sockglue.c in the Linux kernel through 5.1.5. There is an unchecked kmalloc of new_ra, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash).	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4165
1212	CVE-2019-12380	Low	MEDIUM	An issue was discovered in the efi subsystem in the Linux kernel through 5.1.5. phys_efi_set_virtual_address_map in arch/x86/platform/efi/efi.c and efi_call_phys_prolog in arch/x86/platform/efi/efi_64.c mishandle memory allocation failures.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.14	Not vulnerable	Not vulnerable	LIN1018-4164
1213	CVE-2019-12379	Medium	MEDIUM	An issue was discovered in con_insert_unipair in drivers/tty/vt/consolemap.c in the Linux kernel through 5.1.5. There is a memory leak in a certain case of an ENOMEM outcome of kmalloc.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4163
1214	CVE-2019-12378	High	CRITICAL	An issue was discovered in ip6_ra_control in net/ipv6/ipv6_sockglue.c in the Linux kernel through 5.1.5. There is an unchecked kmalloc of new_ra, which might allow an attacker to cause a denial of service (NULL pointer dereference and system crash). NOTE: This has been disputed as not an issue.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4162
1215	CVE-2019-12295	Medium	HIGH	In Wireshark 3.0.0 to 3.0.1, 2.6.0 to 2.6.8, and 2.4.0 to 2.4.14, the dissection engine could crash. This was addressed in epan/packet.c by restricting the number of layers and consequently limiting recursion.	wireshark	Unchanged	8.0.0.31	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4136
1216	CVE-2019-12293	Medium	HIGH	In Poppler through 0.76.1, there is a heap-based buffer over-read in JPXStream::init in JPEG2000Stream.cc via data with inconsistent heights or widths.	poppler	Unchanged	Won't Fix	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4142
1217	CVE-2019-12290	MEDIUM	HIGH	GNU libidn2 before 2.2.0 fails to perform the roundtrip checks specified in RFC3490 Section 4.2 when converting A-labels to U-labels. This makes it possible in some circumstances for one domain to impersonate another. By creating a malicious domain that matches a target domain except for the inclusion of certain punycoded Unicode characters (that would be discarded when converted first to a Unicode label and then back to an ASCII label), arbitrary domains can be impersonated.	libidn2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Vulnerable	Not vulnerable	Investigate	LIN1018-5154
1218	CVE-2019-12222	Medium	MEDIUM	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9. There is an out-of-bounds read in the function SDL_InvalidateMap at video/SDL_pixels.c.	libsdl2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4103
1219	CVE-2019-12221	Medium	MEDIUM	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a SEGV in the SDL function SDL_free_REAL at stdlib/SDL_malloc.c.	libsdl2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4104

	A	B	C	D	E	F	G	H	I	J	K	L	M
1220	CVE-2019-12220	Medium	MEDIUM	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is an out-of-bounds read in the SDL function SDL_FreePalette_REAL at video/SDL_pixels.c.	libsdl2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4105
1221	CVE-2019-12219	Medium	HIGH	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is an invalid free error in the SDL function SDL_SetError_REAL at SDL_error.c.	libsdl2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4106
1222	CVE-2019-12218	Medium	MEDIUM	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a NULL pointer dereference in the SDL2_image function IMG_LoadPCX_RW at IMG_pcx.c.	libsdl2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4107
1223	CVE-2019-12217	Medium	MEDIUM	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a NULL pointer dereference in the SDL stdio_read function in file/SDL_rwops.c.	libsdl2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4108
1224	CVE-2019-12216	Medium	MEDIUM	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9 when used in conjunction with libSDL2_image.a in SDL2_image 2.0.4. There is a heap-based buffer overflow in the SDL2_image function IMG_LoadPCX_RW at IMG_pcx.c.	libsdl2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4109
1225	CVE-2019-12208	High	CRITICAL	njs through 0.3.1, used in NGINX, has a heap-based buffer overflow in njs_function_native_call in njs/njs_function.c.	nginx	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4110
1226	CVE-2019-12207	High	CRITICAL	njs through 0.3.1, used in NGINX, has a heap-based buffer over-read in nxt_utf8_decode in nxt/nxt_utf8.c.	nginx	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4111
1227	CVE-2019-12206	High	CRITICAL	njs through 0.3.1, used in NGINX, has a heap-based buffer overflow in nxt_utf8_encode in nxt_utf8.c.	nginx	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4112
1228	CVE-2019-12155	Medium	HIGH	interface_release_resource in hw/display/qxl.c in QEMU 4.0.0 has a NULL pointer dereference.	qemu	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4150
1229	CVE-2019-12111	Medium	HIGH	A Denial Of Service vulnerability in MiniUPnP MiniUPnPd through 2.1 exists due to a NULL pointer dereference in copyIPv6IfDifferent in pcpserver.c.	miniupnpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4127
1230	CVE-2019-12110	Medium	HIGH	An AddPortMapping Denial Of Service vulnerability in MiniUPnP MiniUPnPd through 2.1 exists due to a NULL pointer dereference in upnpredirect.c.	miniupnpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4126
1231	CVE-2019-12109	Medium	HIGH	A Denial Of Service vulnerability in MiniUPnP MiniUPnPd through 2.1 exists due to a NULL pointer dereference in GetOutboundPinholeTimeout in upnpsoap.c for rem_port.	miniupnpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4125
1232	CVE-2019-12108	Medium	HIGH	A Denial Of Service vulnerability in MiniUPnP MiniUPnPd through 2.1 exists due to a NULL pointer dereference in GetOutboundPinholeTimeout in upnpsoap.c for int_port.	miniupnpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4124
1233	CVE-2019-12107	Medium	HIGH	The upnp_event_prepare function in upnpevents.c in MiniUPnP MiniUPnPd through 2.1 allows a remote attacker to leak information from the heap due to improper validation of an snprintf return value.	miniupnpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4123
1234	CVE-2019-12068	Medium	HIGH	In QEMU 1:4.1-1, 1:2.1+dfsg-12+deb8u6, 1:2.8+dfsg-6+deb9u8, 1:3.1+dfsg-8~deb10u1, 1:3.1+dfsg-8+deb10u2, and 1:2.1+dfsg-12+deb8u12 (fixed), when executing script in lsi_execute_script(), the LSI scsi adapter emulator advances 's->dsp' index to read next opcode. This can lead to an infinite loop if the next opcode is empty. Move the existing loop exit after 10k iterations so that it covers no-op opcodes as well.	qemu	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	10.19.45.1	Not vulnerable	LIN1018-5045
1235	CVE-2019-11884	Low	LOW	The do_hidp_sock_ioctl function in net/bluetooth/hidp/sock.c in the Linux kernel before 5.0.15 allows a local user to obtain potentially sensitive information from kernel stack memory via a HIDPCONNADD command, because a name field may not end with a '\0' character.	linux	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-4061
1236	CVE-2019-11873	High	CRITICAL	wolfSSL 4.0.0 has a Buffer Overflow in DoPreSharedKeys in tls13.c when a current identity size is greater than a client identity size. An attacker sends a crafted hello client packet over the network to a TLSv1.3 wolfSSL server. The length fields of the packet: record length, client hello length, total extensions length, PSK extension length, total identity length, and identity length contain their maximum value which is 2^16. The identity data field of the PSK extension of the packet contains the attack data, to be stored in the undefined memory (RAM) of the server. The size of the data is about 65 kB. Possibly the attacker can perform a remote code execution attack.	wolfssl	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4143
1237	CVE-2019-11833	LOW	MEDIUM	fs/ext4/extents.c in the Linux kernel through 5.1.2 does not zero out the unused memory region in the extent tree block, which might allow local users to obtain sensitive information by reading uninitialized data in the filesystem.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4080
1238	CVE-2019-11815	High	HIGH	An issue was discovered in rds_tcp_kill_sock in net/rds/tcp.c in the Linux kernel before 5.0.8. There is a race condition leading to a use-after-free, related to net namespace cleanup.	linux	Unchanged	Not vulnerable	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-4051
1239	CVE-2019-11811	High	CRITICAL	An issue was discovered in the Linux kernel before 5.0.4. There is a use-after-free upon attempted read access to /proc/ioports after the ipmi_si module is removed, related to drivers/char/ipmi/ipmi_si_intf.c, drivers/char/ipmi/ipmi_si_mem_io.c, and drivers/char/ipmi/ipmi_si_port_io.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-4037
1240	CVE-2019-11810	High	HIGH	An issue was discovered in the Linux kernel before 5.0.7. A NULL pointer dereference can occur when megasas_create_frame_pool() fails in megasas_alloc_cmds() in drivers/scsi/megaraid/megaraid_sas_base.c. This causes a Denial of Service, related to a use-after-free.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-4038

	A	B	C	D	E	F	G	H	I	J	K	L	M
1241	CVE-2019-11779	Medium	MEDIUM	In Eclipse Mosquitto 1.5.0 to 1.6.5 inclusive, if a malicious MQTT client sends a SUBSCRIBE packet containing a topic that consists of approximately 65400 or more '/' characters, i.e. the topic hierarchy separator, then a stack overflow will occur.	mosquitto	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5053
1242	CVE-2019-11768	High	CRITICAL	An issue was discovered in phpMyAdmin before 4.9.0.1. A vulnerability was reported where a specially crafted database name can be used to trigger an SQL injection attack through the designer feature.	phpmyadmin	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4244
1243	CVE-2019-11766	High	CRITICAL	dhcp6.c in dhcpcd before 6.11.7 and 7.x before 7.2.2 has a buffer over-read in the D6_OPTION_PD_EXCLUDE feature.	dhcpcd	Unchanged	Not vulnerable	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3959
1244	CVE-2019-11690	Medium	MEDIUM	gen_rand_uuid in lib/uuid.c in Das U-Boot v2014.04 through v2019.04 lacks an srand call, which allows attackers to determine UUID values in scenarios where CONFIG_RANDOM_UUID is enabled, and Das U-Boot is relied upon for UUID values of a GUID Partition Table of a boot device.	u-boot	Unchanged	Not vulnerable	Not vulnerable	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3964
1245	CVE-2019-11683	High	CRITICAL	udp_gro_receive_segment in net/ipv4/udp_offload.c in the Linux kernel 5.x before 5.0.13 allows remote attackers to cause a denial of service (slab-out-of-bounds memory corruption) or possibly have unspecified other impact via UDP packets with a 0 payload, because of mishandling of padded packets, aka the GRO packet of death issue.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4044
1246	CVE-2019-11599	Medium	HIGH	The coredump implementation in the Linux kernel before 5.0.10 does not use locking or other mechanisms to prevent vma layout or vma flags changes while it runs, which allows local users to obtain sensitive information, cause a denial of service, or possibly have unspecified other impact by triggering a race condition with mmget_not_zero or get_task_mm calls. This is related to fs/userfaultfd.c, mm/mmap.c, fs/proc/task_mmu.c, and drivers/infiniband/core/uverbs_main.c.	linux	Unchanged	Not vulnerable	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3955
1247	CVE-2019-11598	Medium	HIGH	In ImageMagick 7.0.8-40 Q16, there is a heap-based buffer over-read in the function WritePNMImage of coders/pnm.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file. This is related to SetGrayscaleImage in MagickCore/quantize.c.	imagemagick	Unchanged	8.0.0.31	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3953
1248	CVE-2019-11597	Medium	HIGH	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file.	imagemagick	Unchanged	8.0.0.31	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3954
1249	CVE-2019-11579	Medium	MEDIUM	dhcp.c in dhcpcd before 7.2.1 contains a 1-byte read overflow with DHO_OPTSOVERLOADED.	dhcpcd	Unchanged	Not vulnerable	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3956
1250	CVE-2019-11578	Medium	MEDIUM	auth.c in dhcpcd before 7.2.1 allowed attackers to infer secrets by performing latency attacks.	dhcpcd	Unchanged	Not vulnerable	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3957
1251	CVE-2019-11577	High	CRITICAL	dhcpcd before 7.2.1 contains a buffer overflow in dhcp6_findna in dhcp6.c when reading NA/TA addresses.	dhcpcd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3958
1252	CVE-2019-11555	Medium	MEDIUM	The EAP-pwd implementation in hostapd (EAP server) before 2.8 and wpa_supplicant (EAP peer) before 2.8 does not validate fragmentation reassembly state properly for a case where an unexpected fragment could be received. This could result in process termination due to a NULL pointer dereference (denial of service). This affects eap_server/eap_server_pwd.c and eap_peer/eap_pwd.c.	hostapd&wpa-supplicant	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4027
1253	CVE-2019-11500	HIGH	CRITICAL	In Dovecot before 2.2.36.4 and 2.3.x before 2.3.7.2 (and Pigeonhole before 0.5.7.2), protocol processing can fail for quoted strings. This occurs because '\0' characters are mishandled, and can lead to out-of-bounds writes and remote code execution.	dovecot	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4799
1254	CVE-2019-11499	Medium	HIGH	In the IMAP Server in Dovecot 2.3.3 through 2.3.5.2, the submission-login component crashes if AUTH PLAIN is attempted over a TLS secured channel with an unacceptable authentication message.	dovecot	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4049
1255	CVE-2019-11498	Medium	MEDIUM	WavpackSetConfiguration64 in pack_utils.c in libwavpack.a in WavPack through 5.1.0 has a Conditional jump or move depends on uninitialised value condition, which might allow attackers to cause a denial of service (application crash) via a DFF file that lacks valid sample-rate data.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3967
1256	CVE-2019-11494	Medium	HIGH	In the IMAP Server in Dovecot 2.3.3 through 2.3.5.2, the submission-login service crashes when the client disconnects prematurely during the AUTH command.	dovecot	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4050
1257	CVE-2019-11487	High	HIGH	The Linux kernel before 5.1-rc5 allows page->_refcount reference count overflow, with resultant use-after-free issues, if about 140 GiB of RAM exists. This is related to fs/fuse/dev.c, fs/pipe.c, fs/splice.c, include/linux/mm.h, include/linux/pipe_fs_i.h, kernel/trace/trace.c, mm/gup.c, and mm/hugetlb.c. It can occur with FUSE requests.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4045
1258	CVE-2019-11486	Medium	HIGH	The Siemens R3964 line discipline driver in drivers/tty/n_r3964.c in the Linux kernel before 5.0.8 has multiple race conditions.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4331
1259	CVE-2019-11479	Medium	HIGH	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4296

	A	B	C	D	E	F	G	H	I	J	K	L	M
1260	CVE-2019-11478	Medium	HIGH	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4295
1261	CVE-2019-11477	High	HIGH	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4294
1262	CVE-2019-11472	Medium	MEDIUM	ReadXWDImage in coders/xwd.c in the XWD image parsing component of ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (divide-by-zero error) by crafting an XWD image file in which the header indicates neither LSB first nor MSB first.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3933
1263	CVE-2019-11470	High	MEDIUM	The cineon parsing component in ImageMagick 7.0.8-26 Q16 allows attackers to cause a denial-of-service (uncontrolled resource consumption) by crafting a Cineon image with an incorrect claimed image size. This occurs because ReadCINImage in coders/cin.c lacks a check for insufficient image data in a file.	imagemagick	Unchanged	8.0.0.31	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3940
1264	CVE-2019-11463	Medium	MEDIUM	A memory leak in archive_read_format_zip_cleanup in archive_read_support_format_zip.c in libarchive 3.3.4-dev allows remote attackers to cause a denial of service via a crafted ZIP file because of a HAVE_LZMA_H typo. NOTE: this only affects users who downloaded the development code from GitHub. Users of the product's official releases are unaffected.	libarchive	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3968
1265	CVE-2019-11461	Medium	HIGH	An issue was discovered in GNOME Nautilus 3.30 prior to 3.30.6 and 3.32 prior to 3.32.1. A compromised thumbnailer may escape the bubblewrap sandbox used to confine thumbnailers by using the TIOCSTI ioctl to push characters into the input buffer of the thumbnailer's controlling terminal, allowing an attacker to escape the sandbox if the thumbnailer has a controlling terminal. This is due to improper filtering of the TIOCSTI ioctl on 64-bit systems, similar to CVE-2019-10063.	nautilus	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-8408
1266	CVE-2019-11460	Medium	CRITICAL	An issue was discovered in GNOME gnome-desktop 3.26, 3.28, and 3.30 prior to 3.30.2.2, and 3.32 prior to 3.32.1.1. A compromised thumbnailer may escape the bubblewrap sandbox used to confine thumbnailers by using the TIOCSTI ioctl to push characters into the input buffer of the thumbnailer's controlling terminal, allowing an attacker to escape the sandbox if the thumbnailer has a controlling terminal. This is due to improper filtering of the TIOCSTI ioctl on 64-bit systems, similar to CVE-2019-10063.	gnome-desktop	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4022
1267	CVE-2019-11459	Medium	MEDIUM	The tiff_document_render() and tiff_document_get_thumbnail() functions in the TIFF document backend in GNOME Evince through 3.32.0 did not handle errors from TIFFReadRGBAImageOriented(), leading to uninitialized memory use when processing certain TIFF image files.	evince	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4024
1268	CVE-2019-11455	Medium	HIGH	A buffer over-read in Util_urlDecode in util.c in Tildeslash Monit before 5.25.3 allows a remote authenticated attacker to retrieve the contents of adjacent memory via manipulation of GET or POST parameters. The attacker can also cause a denial of service (application outage).	monit	Unchanged	Won't Fix	Won't Fix	10.17.41.17	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4028
1269	CVE-2019-11454	Medium	MEDIUM	Persistent cross-site scripting (XSS) in http/cervlet.c in Tildeslash Monit before 5.25.3 allows a remote unauthenticated attacker to introduce arbitrary JavaScript via manipulation of an unsanitized user field of the Authorization header for HTTP Basic Authentication, which is mishandled during an _viewlog operation.	monit	Unchanged	Won't Fix	Won't Fix	10.17.41.17	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3965
1270	CVE-2019-11393	Medium	CRITICAL	An issue was discovered in /admin/users/update in M/Monit before 3.7.3. It allows unprivileged users to escalate their privileges to an administrator by requesting a password change and specifying the admin parameter.	monit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3966
1271	CVE-2019-11366	Medium	MEDIUM	An issue was discovered in atftpd in atftp 0.7.1. It does not lock the thread_list_mutex mutex before assigning the current thread data structure. As a result, the daemon is vulnerable to a denial of service attack due to a NULL pointer dereference. If thread_data is NULL when assigned to current, and modified by another thread before a certain tftpd_list.c check, there is a crash when dereferencing current->next.	atftp	Unchanged	8.0.0.31	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3970
1272	CVE-2019-11365	High	CRITICAL	An issue was discovered in atftpd in atftp 0.7.1. A remote attacker may send a crafted packet triggering a stack-based buffer overflow due to an insecurely implemented strncpy call. The vulnerability is triggered by sending an error packet of 3 bytes or fewer. There are multiple instances of this vulnerable strncpy pattern within the code base, specifically within tftpd_file.c, tftp_file.c, tftpd_mtftp.c, and tftp_mtftp.c.	atftp	Unchanged	8.0.0.31	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3971
1273	CVE-2019-11360	Medium	MEDIUM	A buffer overflow in iptables-restore in netfilter iptables 1.8.2 allows an attacker to (at least) crash the program or potentially gain code execution via a specially crafted iptables-save file. This is related to add_param_to_argv in xshared.c.	iptables	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4443

	A	B	C	D	E	F	G	H	I	J	K	L	M
1274	CVE-2019-11339	Medium	HIGH	The studio profile decoder in libavcodec/mpeg4videodec.c in FFmpeg 4.0 before 4.0.4 and 4.1 before 4.1.2 allows remote attackers to cause a denial of service (out-of-array access) or possibly have unspecified other impact via crafted MPEG-4 video data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3915
1275	CVE-2019-11338	Medium	HIGH	libavcodec/hevcdec.c in FFmpeg 4.1.2 mishandles detection of duplicate first slices, which allows remote attackers to cause a denial of service (NULL pointer dereference and out-of-array access) or possibly have unspecified other impact via crafted HEVC data.	ffmpeg	Unchanged	Won't Fix	9.0.0.21	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3916
1276	CVE-2019-11328	High	HIGH	An issue was discovered in Singularity 3.1.0 to 3.2.0-rc2, a malicious user with local/network access to the host system (e.g. ssh) could exploit this vulnerability due to insecure permissions allowing a user to edit files within `/run/singularity/instances/sing/<user>/<instance>`. The manipulation of those files can change the behavior of the starter-suid program when instances are joined resulting in potential privilege escalation on the host.	singularity	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4154
1277	CVE-2019-11324	Medium	HIGH	The urllib3 library before 1.24.2 for Python mishandles certain cases where the desired set of CA certificates is different from the OS store of CA certificates, which results in SSL connections succeeding in situations where a verification failure is the correct outcome. This is related to use of the ssl_context, ca_certs, or ca_certs_dir argument.	python-urllib3	Unchanged	Won't Fix	Won't Fix	Vulnerable	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3972
1278	CVE-2019-11255	MEDIUM	MEDIUM	Improper input validation in Kubernetes CSI sidecar containers for external-provisioner (<v0.4.3, <v1.0.2, v1.1, <v1.2.2, <v1.3.1), external-snapshotter (<v0.4.2, <v1.0.2, v1.1, <1.2.2), and external-resizer (v0.1, v0.2) could result in unauthorized PersistentVolume data access or volume mutation during snapshot, restore from snapshot, cloning and resizing operations.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Investigate	Investigate	LIN1019-3725
1279	CVE-2019-11254	MEDIUM	MEDIUM	The Kubernetes API Server component in versions 1.1-1.14, and versions prior to 1.15.10, 1.16.7 and 1.17.3 allows an authorized user who sends malicious YAML payloads to cause the kube-apiserver to consume excessive CPU cycles while parsing YAML.	kubernetes	Updated	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Investigate	Investigate	LIN1019-4220
1280	CVE-2019-11251	MEDIUM	MEDIUM	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	kubernetes	Updated	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	10.19.45.5	10.20.15.0	LIN1019-4047
1281	CVE-2019-11250	LOW	MEDIUM	The Kubernetes client-go library logs request headers at verbosity levels of 7 or higher. This can disclose credentials to unauthorized users via logs or command output. Kubernetes components (such as kube-apiserver) prior to v1.16.0, which make use of basic or bearer token authentication, and run at high verbosity levels, are affected.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4800
1282	CVE-2019-1125	Low	MEDIUM	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073.	linux	Unchanged	8.0.0.31	9.0.0.25	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4938
1283	CVE-2019-11249	MEDIUM	MEDIUM	The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Kubernetes runs tar inside the container to create a tar archive, copies it over the network, and kubectl unpacks it on the user?s machine. If the tar binary in the container is malicious, it could run any code and output unexpected, malicious results. An attacker could use this to write files to any path on the user?s machine when kubectl cp is called, limited only by the system permissions of the local user. Kubernetes affected versions include versions prior to 1.13.9, versions prior to 1.14.5, versions prior to 1.15.2, and versions 1.1, 1.2, 1.4, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11, 1.12.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4801
1284	CVE-2019-11247	MEDIUM	HIGH	The Kubernetes kube-apiserver mistakenly allows access to a cluster-scoped custom resource if the request is made as if the resource were namespaced. Authorizations for the resource accessed in this manner are enforced using roles and role bindings within the namespace, meaning that a user with access only to a resource in one namespace could create, view update or delete the cluster-scoped resource (according to their namespace role privileges). Kubernetes affected versions include versions prior to 1.13.9, versions prior to 1.14.5, versions prior to 1.15.2, and versions 1.7, 1.8, 1.9, 1.10, 1.11, 1.12.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4803
1285	CVE-2019-11246	MEDIUM	MEDIUM	The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Kubernetes runs tar inside the container to create a tar archive, copies it over the network, and kubectl unpacks it on the user?s machine. If the tar binary in the container is malicious, it could run any code and output unexpected, malicious results. An attacker could use this to write files to any path on the user?s machine when kubectl cp is called, limited only by the system permissions of the local user. Kubernetes affected versions include versions prior to 1.12.9, versions prior to 1.13.6, versions prior to 1.14.2, and versions 1.1, 1.2, 1.4, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4804

	A	B	C	D	E	F	G	H	I	J	K	L	M
1286	CVE-2019-11244	Low	MEDIUM	In Kubernetes v1.8.x-v1.14.x, schema info is cached by kubectl in the location specified by --cache-dir (defaulting to $HOME/.kube/http-cache), written with world-writeable permissions (rw-rw-rw-). If --cache-dir is specified and pointed at a different location accessible to other users/groups, the written files may be modified by other users/groups and disrupt the kubectl invocation.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3941
1287	CVE-2019-11243	Medium	HIGH	In Kubernetes v1.12.0-v1.12.4 and v1.13.0, the rest.AnonymousClientConfig() method returns a copy of the provided config, with credentials removed (bearer token, username/password, and client certificate/key data). In the affected versions, rest.AnonymousClientConfig() did not effectively clear service account credentials loaded using rest.InClusterConfig()	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3988
1288	CVE-2019-11235	High	CRITICAL	FreeRADIUS before 3.0.19 mishandles the each participant verifies that the received scalar is within a range, and that the received group element is a valid point on the curve being used protection mechanism, aka a Dragonblood issue, a similar issue to CVE-2019-9498 and CVE-2019-9499.	freeradius	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3973
1289	CVE-2019-11234	High	CRITICAL	FreeRADIUS before 3.0.19 does not prevent use of reflection for authenticon spoofing, aka a Dragonblood issue, a similar issue to CVE-2019-9497.	freeradius	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3974
1290	CVE-2019-11191	Medium	MEDIUM	The Linux kernel through 5.0.7, when CONFIG_IA32_AOUT is enabled and ia32_aout is loaded, allows local users to bypass ASLR on setuid a.out programs (if any exist) because install_exec_creds() is called too late in load_aout_binary() in fs/binfmt_aout.c, and thus the ptrace_may_access() check has a race condition when reading /proc/pid/stat.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-3902
1291	CVE-2019-11190	Medium	MEDIUM	The Linux kernel before 4.8 allows local users to bypass ASLR on setuid programs (such as /bin/su) because install_exec_creds() is called too late in load_elf_binary() in fs/binfmt_elf.c, and thus the ptrace_may_access() check has a race condition when reading /proc/pid/stat.	linux	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3903
1292	CVE-2019-11139	LOW	MEDIUM	Improper conditions check in the voltage modulation interface for some Intel(R) Xeon(R) Scalable Processors may allow a privileged user to potentially enable denial of service via local access.	microcode	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Won't Fix	LIN1019-3466
1293	CVE-2019-11135	LOW	MEDIUM	TSX Asynchronous Abort condition on some CPUs utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.	microcode	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Won't Fix	LIN1019-3465
1294	CVE-2019-11091	Medium	MEDIUM	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.17	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-4078
1295	CVE-2019-11085	Medium	HIGH	Insufficient input validation in Kernel Mode Driver in Intel(R) i915 Graphics for Linux before version 5.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4330
1296	CVE-2019-11072	High	CRITICAL	lighttpd before 1.4.54 has a signed integer overflow, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a malicious HTTP GET request, as demonstrated by mishandling of /%2F? in burl_normalize_2F_to_slash_fix in burl.c.	lighttpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3900
1297	CVE-2019-11068	High	CRITICAL	libxslt through 1.1.33 allows bypass of a protection mechanism because callers of xsltCheckRead and xsltCheckWrite permit access even upon receiving a -1 error code. xsltCheckRead can return -1 for a crafted URL that is not actually invalid and is subsequently loaded.	libxslt	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3899
1298	CVE-2019-11059	High	CRITICAL	Das U-Boot 2016.11-rc1 through 2019.04 mishandles the ext4 64-bit extension, resulting in a buffer overflow.	u-boot	Unchanged	Not vulnerable	Not vulnerable	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4062
1299	CVE-2019-11050	MEDIUM	MEDIUM	When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	None	LIN1019-3827
1300	CVE-2019-11049	HIGH	CRITICAL	In PHP versions 7.3.x below 7.3.13 and 7.4.0 on Windows, when supplying custom headers to mail() function, due to mistake introduced in commit 7bf4b4a2dcf92ddbccea1bb95f8390a18ac3342e, if the header is supplied in lowercase, this can result in double-freeing certain memory locations.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.19.45.3	Investigate	LIN1019-3828
1301	CVE-2019-11047	MEDIUM	MEDIUM	When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	None	LIN1019-3829
1302	CVE-2019-11046	MEDIUM	HIGH	In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0, PHP bcmath extension functions on some systems, including Windows, can be tricked into reading beyond the allocated space by supplying it with string containing characters that are identified as numeric by the OS but aren't ASCII numbers. This can read to disclosure of the content of some memory locations.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	None	LIN1019-3830

	A	B	C	D	E	F	G	H	I	J	K	L	M
1303	CVE-2019-11045	MEDIUM	MEDIUM	In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0, PHP DirectoryIterator class accepts filenames with embedded \0 byte and treats them as terminating at that byte. This could lead to security vulnerabilities, e.g. in applications checking paths that the code is allowed to access.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	None	LIN1019-3831
1304	CVE-2019-11044	MEDIUM	HIGH	In PHP versions 7.2.x below 7.2.26, 7.3.x below 7.3.13 and 7.4.0 on Windows, PHP link() function accepts filenames with embedded \0 byte and treats them as terminating at that byte. This could lead to security vulnerabilities, e.g. in applications checking paths that the code is allowed to access.	php	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	10.19.45.3	Investigate	LIN1019-3832
1305	CVE-2019-11043	HIGH	CRITICAL	In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.	php	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Investigate	Not vulnerable	LIN1018-5176
1306	CVE-2019-11042	MEDIUM	HIGH	When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.31, 7.2.x below 7.2.21 and 7.3.x below 7.3.8 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.31	9.0.0.22	10.17.41.18	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4643
1307	CVE-2019-11041	MEDIUM	HIGH	When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.31, 7.2.x below 7.2.21 and 7.3.x below 7.3.8 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.31	9.0.0.22	10.17.41.18	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4644
1308	CVE-2019-11040	Medium	CRITICAL	When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4303
1309	CVE-2019-11039	Medium	CRITICAL	Function iconv_mime_decode_headers() in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 may perform out-of-buffer read due to integer overflow when parsing MIME headers. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4301
1310	CVE-2019-11038	Medium	MEDIUM	When using gdImageCreateFromXbm() function of PHP gd extension in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6, it is possible to supply data that will cause the function to use the value of uninitialized variable. This may lead to disclosing contents of the stack that has been left there by previous code.	php	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4302
1311	CVE-2019-11037	High	CRITICAL	In PHP imagick extension in versions between 3.3.0 and 3.4.4, writing to an array of values in ImagickKernel::fromMatrix() function did not check that the address will be within the allocated array. This could lead to out of bounds write to memory if the function is called with the data controlled by untrusted party.	php	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-3975
1312	CVE-2019-11036	Medium	CRITICAL	When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.29, 7.2.x below 7.2.18 and 7.3.x below 7.3.5 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3976
1313	CVE-2019-11035	Medium	CRITICAL	When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_iif_add_value function. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3977
1314	CVE-2019-11034	Medium	CRITICAL	When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.	php	Unchanged	8.0.0.31	9.0.0.21	10.17.41.16	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-3978
1315	CVE-2019-11026	Medium	MEDIUM	FontInfoScanner::scanFonts in FontInfo.cc in Poppler 0.75.0 has infinite recursion, leading to a call to the error function in Error.cc.	poppler	Unchanged	Won't Fix	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3888
1316	CVE-2019-10903	Medium	HIGH	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the DCERPC SPOOLSS dissector could crash. This was addressed in epan/dissectors/packet-dcerpc-spoolss.c by adding a boundary check.	wireshark	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3862
1317	CVE-2019-10902	Medium	HIGH	In Wireshark 3.0.0, the TSDNS dissector could crash. This was addressed in epan/dissectors/packet-tsdns.c by splitting strings safely.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3863
1318	CVE-2019-10901	Medium	HIGH	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the LDSS dissector could crash. This was addressed in epan/dissectors/packet-ldss.c by handling file digests properly.	wireshark	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3864
1319	CVE-2019-10900	Medium	HIGH	In Wireshark 3.0.0, the Rbm dissector could go into an infinite loop. This was addressed in epan/dissectors/file-rbm.c by handling unknown object types safely.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3865
1320	CVE-2019-10899	Medium	HIGH	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the SRVLOC dissector could crash. This was addressed in epan/dissectors/packet-srvloc.c by preventing a heap-based buffer under-read.	wireshark	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3866
1321	CVE-2019-10898	Medium	HIGH	In Wireshark 3.0.0, the GSUP dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-gsm_gsup.c by rejecting an invalid Information Element length.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3867
1322	CVE-2019-10897	Medium	HIGH	In Wireshark 3.0.0, the IEEE 802.11 dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-ieee80211.c by detecting cases in which the bit offset does not advance.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3868

	A	B	C	D	E	F	G	H	I	J	K	L	M
1323	CVE-2019-10896	Medium	HIGH	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the DOF dissector could crash. This was addressed in epan/dissectors/packet-dof.c by properly handling generated IID and OID bytes.	wireshark	Unchanged	Not vulnerable	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3869
1324	CVE-2019-10895	Medium	HIGH	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the NetScaler file parser could crash. This was addressed in wiretap/netscaler.c by improving data validation.	wireshark	Unchanged	Vulnerable	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3870
1325	CVE-2019-10894	Medium	HIGH	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the GSS-API dissector could crash. This was addressed in epan/dissectors/packet-gssapi.c by ensuring that a valid dissector is called.	wireshark	Unchanged	Not vulnerable	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3871
1326	CVE-2019-10874	Medium	HIGH	Cross Site Request Forgery (CSRF) in the bolt/upload File Upload feature in Bolt CMS 3.6.6 allows remote attackers to execute arbitrary code by uploading a JavaScript file to include executable extensions in the file/edit/config/config.yml configuration file.	bolt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10760
1327	CVE-2019-10873	Medium	MEDIUM	An issue was discovered in Poppler 0.74.0. There is a NULL pointer dereference in the function SplashClip::clipAALine at splash/SplashClip.cc.	poppler	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3836
1328	CVE-2019-10872	Medium	HIGH	An issue was discovered in Poppler 0.74.0. There is a heap-based buffer over-read in the function Splash::blitTransparent at splash/Splash.cc.	poppler	Unchanged	Won't Fix	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3844
1329	CVE-2019-10871	Medium	MEDIUM	An issue was discovered in Poppler 0.74.0. There is a heap-based buffer over-read in the function PSOutputDev::checkPageSlice at PSOutputDev.cc.	poppler	Unchanged	Won't Fix	9.0.0.24	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3845
1330	CVE-2019-10714	Medium	MEDIUM	LocaleLowercase in MagickCore/locale.c in ImageMagick before 7.0.8-32 allows out-of-bounds access, leading to a SIGSEGV.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3839
1331	CVE-2019-10691	Medium	HIGH	The JSON encoder in Dovecot before 2.3.5.2 allows attackers to repeatedly crash the authentication service by attempting to authenticate with an invalid UTF-8 sequence as the username.	dovecot	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4025
1332	CVE-2019-10654	Medium	MEDIUM	The lzo1x_decompress function in liblzo2.so.2 in LZO 2.10, as used in Long Range Zip (aka lrzip) 0.631, allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted archive, a different vulnerability than CVE-2017-8845.	lzo	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-3855
1333	CVE-2019-10650	Medium	HIGH	In ImageMagick 7.0.8-36 Q16, there is a heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c, which allows an attacker to cause a denial of service or information disclosure via a crafted image file.	imagemagick	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3840
1334	CVE-2019-10649	Medium	MEDIUM	In ImageMagick 7.0.8-36 Q16, there is a memory leak in the function SVGKeyValuePairs of coders/svg.c, which allows an attacker to cause a denial of service via a crafted image file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3841
1335	CVE-2019-10639	MEDIUM	HIGH	The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel address disclosure), leading to a KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key contains enough bits from a kernel address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is exposed. This attack can be carried out remotely, by the attacker forcing the target device to send UDP or ICMP (or certain other) traffic to attacker-controlled IP addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if the server answers ICMP Echo requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can be used to force UDP traffic to attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because IP ID generation was changed to have a dependency on an address associated with a network namespace.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4411
1336	CVE-2019-10638	Medium	MEDIUM	In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conducted by hosting a crafted web page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4412
1337	CVE-2019-10222	MEDIUM	HIGH	A flaw was found in the Ceph RGW configuration with Beast as the front end handling client requests. An unauthenticated attacker could crash the Ceph RGW server by sending valid HTTP headers and terminating the connection, resulting in a remote denial of service for Ceph RGW clients.	ceph	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	LIN1019-3469
1338	CVE-2019-10220	HIGH	HIGH	Linux kernel CIFS implementation, version 4.9.0 is vulnerable to a relative paths injection in directory entry lists.	linux	Unchanged	Vulnerable	9.0.0.25	10.17.41.20	10.18.44.14	10.19.45.2	10.20.3.0	LIN1019-3666
1339	CVE-2019-10218	MEDIUM	MEDIUM	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.	samba	Unchanged	Investigate	Investigate	10.17.41.19	10.18.44.12	10.19.45.2	Not vulnerable	LIN1019-3297

	A	B	C	D	E	F	G	H	I	J	K	L	M
1340	CVE-2019-10208	MEDIUM	HIGH	A flaw was discovered in postgresql where arbitrary SQL statements can be executed given a suitable SECURITY DEFINER function. An attacker, with EXECUTE permission on the function, can execute arbitrary SQL as the owner of the function.	postgresql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Investigate	LIN1018-5185
1341	CVE-2019-10207	LOW	MEDIUM	A flaw was found in the Linux kernel's Bluetooth implementation of UART, all versions kernel 3.x.x before 4.18.0 and kernel 5.x.x. An attacker with local access and write permissions to the Bluetooth hardware could use this flaw to issue a specially crafted ioctl function call and cause the system to crash.	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.19	10.18.44.14	Not vulnerable	Not vulnerable	LIN1019-3603
1342	CVE-2019-1020001	MEDIUM	HIGH	yard before 0.9.20 allows path traversal.	yard	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4563
1343	CVE-2019-10197	Medium	CRITICAL	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4834
1344	CVE-2019-10193	MEDIUM	HIGH	A stack-buffer overflow vulnerability was found in the Redis hyperloglog data structure versions 3.x before 3.2.13, 4.x before 4.0.14 and 5.x before 5.0.4. By corrupting a hyperloglog using the SETRANGE command, an attacker could cause Redis to perform controlled increments of up to 12 bytes past the end of a stack-allocated buffer.	redis	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4440
1345	CVE-2019-10192	MEDIUM	HIGH	A heap-buffer overflow vulnerability was found in the Redis hyperloglog data structure versions 3.x before 3.2.13, 4.x before 4.0.14 and 5.x before 5.0.4. By carefully corrupting a hyperloglog using the SETRANGE command, an attacker could trick Redis interpretation of dense HLL encoding to write up to 3 bytes beyond the end of a heap-allocated buffer.	redis	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4444
1346	CVE-2019-10168	Medium	HIGH	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an emulator argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4615
1347	CVE-2019-10167	Medium	HIGH	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an emulatorbin argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges.	libvirt	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4614
1348	CVE-2019-10164	High	HIGH	PostgreSQL versions 10.x before 10.9 and versions 11.x before 11.4 are vulnerable to a stack-based buffer overflow. Any authenticated user can overflow a stack-based buffer by changing the user's own password to a purpose-crafted value. This often suffices to execute arbitrary code as the PostgreSQL operating system account.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4363
1349	CVE-2019-10161	High	HIGH	It was discovered that libvirtd before versions 4.10.1 and 5.4.1 would permit read-only clients to use the virDomainSaveImageGetXMLDesc() API, specifying an arbitrary path which would be accessed with the permissions of the libvirtd process. An attacker with access to the libvirtd socket could use this to probe the existence of arbitrary files, cause denial of service or cause libvirtd to execute arbitrary programs.	libvirt	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4591
1350	CVE-2019-10160	Medium	CRITICAL	A security regression of CVE-2019-9636 was discovered in python since commit d537ab0ff9767ef024f26246899728f0116b1ec3 affecting versions 2.7, 3.5, 3.6, 3.7 and from v3.8.0a4 through v3.8.0b1, which still allows an attacker to exploit CVE-2019-9636 by abusing the user and password parts of a URL. When an application parses user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed. The result of an attack may vary based on the application.	python	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	10.19.45.1	Not vulnerable	LIN1018-4247
1351	CVE-2019-10143	Medium	HIGH	It was discovered freeradius up to and including version 3.0.19 does not correctly configure logrotate, allowing a local attacker who already has control of the radiusd user to escalate his privileges to root, by tricking logrotate into writing a radiusd-writable file to a directory normally inaccessible by the radiusd user.	freeradius	Unchanged	8.0.0.31	Investigate	10.17.41.17	10.18.44.8	10.19.45.1	Not vulnerable	LIN1018-4159
1352	CVE-2019-10142	MEDIUM	HIGH	A flaw was found in the Linux kernel's freescale hypervisor manager implementation, kernel versions 5.0.x up to, excluding 5.0.17. A parameter passed to an ioctl was incorrectly validated and used in size calculations for the page size calculation. An attacker can use this flaw to crash the system, corrupt memory, or create other adverse security affects.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4568
1353	CVE-2019-10132	Medium	HIGH	A vulnerability was found in libvirt >= 4.1.0 in the virtlockd-admin.socket and virtlogd-admin.socket systemd units. A missing SocketMode configuration parameter allows any user on the host to connect using virtlockd-admin-sock or virtlogd-admin-sock and perform administrative tasks against the virtlockd and virtlogd daemons.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4140

	A	B	C	D	E	F	G	H	I	J	K	L	M
1354	CVE-2019-10131	Low	HIGH	An off-by-one read vulnerability was discovered in ImageMagick before version 7.0.7-28 in the formatIPTCfromBuffer function in coders/meta.c. A local attacker may use this flaw to read beyond the end of the buffer or to crash the program.	imagemagick	Unchanged	8.0.0.31	9.0.0.21	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4016
1355	CVE-2019-10130	MEDIUM	MEDIUM	A vulnerability was found in PostgreSQL versions 11.x up to excluding 11.3, 10.x up to excluding 10.8, 9.6.x up to, excluding 9.6.13, 9.5.x up to, excluding 9.5.17. PostgreSQL maintains column statistics for tables. Certain statistics, such as histograms and lists of most common values, contain values taken from the column. PostgreSQL does not evaluate row security policies before consulting those statistics during query planning; an attacker can exploit this to read the most common values of certain columns. Affected columns are those for which the attacker has SELECT privilege and for which, in an ordinary query, row-level security prunes the set of rows visible to the attacker.	postgresql	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4570
1356	CVE-2019-10129	MEDIUM	MEDIUM	A vulnerability was found in postgresql versions 11.x prior to 11.3. Using a purpose-crafted insert to a partitioned table, an attacker can read arbitrary bytes of server memory. In the default configuration, any user can create a partitioned table suitable for this attack. (Exploit prerequisites are the same as for CVE-2018-1052).	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4571
1357	CVE-2019-10126	High	CRITICAL	A flaw was found in the Linux kernel. A heap based buffer overflow in mwifiex_uap_parse_tail_ies function in drivers/net/wireless/marvell/mwifiex/ie.c might lead to memory corruption and possibly other consequences.	linux	Unchanged	Not vulnerable	9.0.0.22	10.17.41.17	10.18.44.9	10.19.45.1	Not vulnerable	LIN1018-4287
1358	CVE-2019-10125	High	CRITICAL	An issue was discovered in aio_poll() in fs/aio.c in the Linux kernel through 5.0.4. A file may be released by aio_poll_wake() if an expected event is triggered immediately (e.g., by the close of a pair of pipes) after the return of vfs_poll(), and this will cause a use-after-free.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3804
1359	CVE-2019-10124	High	HIGH	An issue was discovered in the hwpoison implementation in mm/memory-failure.c in the Linux kernel before 5.0.4. When soft_offline_in_use_page() runs on a thp tail page after pmd is split, an attacker can cause a denial of service (BUG).	linux	Unchanged	Not vulnerable	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3805
1360	CVE-2019-1010319	MEDIUM	MEDIUM	WavPack 5.1.0 and earlier is affected by: CWE-457: Use of Uninitialized Variable. The impact is: Unexpected control flow, crashes, and segfaults. The component is: ParseWave64HeaderConfig (wave64.c:211). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit https://github.com/dbry/WavPack/commit/33a0025d1d63ccd05d9dbaa6923d52b1446a62fe.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4424
1361	CVE-2019-1010317	MEDIUM	MEDIUM	WavPack 5.1.0 and earlier is affected by: CWE-457: Use of Uninitialized Variable. The impact is: Unexpected control flow, crashes, and segfaults. The component is: ParseCaffHeaderConfig (caff.c:486). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit https://github.com/dbry/WavPack/commit/f68a9555b548306c5b1ee45199ccdc4a16a6101b.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4425
1362	CVE-2019-1010315	MEDIUM	MEDIUM	WavPack 5.1 and earlier is affected by: CWE 369: Divide by Zero. The impact is: Divide by zero can lead to sudden crash of a software/service that tries to parse a .wav file. The component is: ParseDsdiffHeaderConfig (dsdiff.c:282). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit https://github.com/dbry/WavPack/commit/4c0faba32fddbd0745cbfaf1e1aeb3da5d35b9fc.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4426
1363	CVE-2019-1010305	MEDIUM	MEDIUM	libmspack 0.9.1alpha is affected by: Buffer Overflow. The impact is: Information Disclosure. The component is: function chmd_read_headers() in libmspack(file libmspack/mspack/chmd.c). The attack vector is: the victim must open a specially crafted chm file. The fixed version is: after commit 2f084136cfe0d05e5bf5703f3e83c6d955234b4d.	libmspack	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4437
1364	CVE-2019-1010279	MEDIUM	HIGH	Open Information Security Foundation Suricata prior to version 4.1.3 is affected by: Denial of Service - TCP/HTTP detection bypass. The impact is: An attacker can evade a signature detection with a specialy formed sequence of network packets. The component is: detect.c (https://github.com/OISF/suricata/pull/3625/commits/d8634daf74c882356659addb65fb142b738a186b). The attack vector is: An attacker can trigger the vulnerability by a specifically crafted network TCP session. The fixed version is: 4.1.3.	suricata	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4559
1365	CVE-2019-1010259	High	CRITICAL	SaltStack Salt 2018.3, 2019.2 is affected by: SQL Injection. The impact is: An attacker could escalate privileges on MySQL server deployed by cloud provider. It leads to RCE. The component is: The mysql.user_chpass function from the MySQL module for Salt (https://github.com/saltstack/salt/blob/develop/salt/modules/mysql.py#L1462). The attack vector is: specially crafted password string. The fixed version is: 2018.3.4.	mysql	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4577

	A	B	C	D	E	F	G	H	I	J	K	L	M
1366	CVE-2019-1010251	Medium	HIGH	Open Information Security Foundation Suricata prior to version 4.1.2 is affected by: Denial of Service - DNS detection bypass. The impact is: An attacker can evade a signature detection with a specialy formed network packet. The component is: app-layer-detect-proto.c, decode.c, decode-teredo.c and decode-ipv6.c (https://github.com/OISF/suricata/pull/3590/commits/11f3659f64a4e42e90cb3c09fcef66894205aefe, https://github.com/OISF/suricata/pull/3590/commits/8357ef3f8ffc7d99ef6571350724160de356158b). The attack vector is: An attacker can trigger the vulnerability by sending a specifically crafted network request. The fixed version is: 4.1.2.	suricata	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4558
1367	CVE-2019-1010238	High	CRITICAL	Gnome Pango 1.42 and later is affected by: Buffer Overflow. The impact is: The heap based buffer overflow can be used to get code execution. The component is: function name: pango_log2vis_get_embedding_levels, assignment of nchars and the loop condition. The attack vector is: Bug can be used when application pass invalid utf-8 strings to functions like pango_itemize.	pango	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-4464
1368	CVE-2019-1010220	Medium	LOW	tcpdump.org tcpdump 4.9.2 is affected by: CWE-126: Buffer Over-read. The impact is: May expose Saved Frame Pointer, Return Address etc. on stack. The component is: line 234: ND_PRINT((ndo, %s, buf));, in function named print_prefix, in print-hncp.c. The attack vector is: The victim must open a specially crafted pcap file.	tcpdump	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4560
1369	CVE-2019-1010218	Medium	HIGH	Cherokee Webserver Latest Cherokee Web server Upto Version 1.2.103 (Current stable) is affected by: Buffer Overflow - CWE-120. The impact is: Crash. The component is: Main cherokee command. The attack vector is: Overwrite argv[0] to an insane length with execl. The fixed version is: There's no fix yet.	cherokee	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4555
1370	CVE-2019-1010204	Medium	MEDIUM	GNU binutils gold gold v1.11-v1.16 (GNU binutils v2.21-v2.31.1) is affected by: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read. The impact is: Denial of service. The component is: gold/fileread.cc:497, elfcpp/elfcpp_file.h:644. The attack vector is: An ELF file with an invalid e_shoff header field must be opened.	binutils	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-4477
1371	CVE-2019-1010180	MEDIUM	HIGH	GNU gdb All versions is affected by: Buffer Overflow - Out of bound memory access. The impact is: Deny of Service, Memory Disclosure, and Possible Code Execution. The component is: The main gdb module. The attack vector is: Open an ELF for debugging. The fixed version is: Not fixed yet.	gdb	Unchanged	8.0.0.31	9.0.0.24	10.17.41.20	10.18.44.11	10.19.45.2	Not vulnerable	LIN1018-4483
1372	CVE-2019-1010142	Medium	HIGH	scapy 2.4.0 is affected by: Denial of Service. The impact is: infinite loop, resource consumption and program unresponsive. The component is: _RADIUSAttrPacketListField.getfield(self,). The attack vector is: over the network or in a pcap. both work.	scapy	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4463
1373	CVE-2019-1010025	MEDIUM	MEDIUM	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4436
1374	CVE-2019-1010024	MEDIUM	MEDIUM	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc.	glibc	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1018-4435
1375	CVE-2019-1010023	MEDIUM	HIGH	GNU Libc current is affected by: Re-mapping current loaded libray with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code.	glibc	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1018-4434
1376	CVE-2019-1010022	HIGH	CRITICAL	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard.	glibc	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1018-4433
1377	CVE-2019-1010006	Medium	HIGH	Evince 3.26.0 is affected by buffer overflow. The impact is: DOS / Possible code execution. The component is: backend/tiff/tiff-document.c. The attack vector is: Victin must open a crafted PDF file.	evince	Unchanged	Won't Fix	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4438
1378	CVE-2019-10098	Medium	MEDIUM	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.	apache	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5011
1379	CVE-2019-10097	Medium	HIGH	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the PROXY protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5010
1380	CVE-2019-10092	Medium	MEDIUM	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.	apache	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5009
1381	CVE-2019-10082	Medium	CRITICAL	In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.	apache	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-5008
1382	CVE-2019-10064	MEDIUM	HIGH	hostapd before 2.6, in EAP mode, makes calls to the rand() and random() standard library functions without any preceding srand() or srandom() call, which results in inappropriate use of deterministic values. This was fixed in conjunction with CVE-2016-10743.	hostapd&wpa-supplicant	Unchanged	8.0.0.33	9.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1019-4098

	A	B	C	D	E	F	G	H	I	J	K	L	M
1383	CVE-2019-10061	HIGH	CRITICAL	utils/find-opencv.js in node-opencv (aka OpenCV bindings for Node.js) prior to 6.1.0 is vulnerable to Command Injection. It does not validate user input allowing attackers to execute arbitrary commands.	opencv	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3797
1384	CVE-2019-10056	MEDIUM	HIGH	An issue was discovered in Suricata 4.1.3. The code mishandles the case of sending a network packet with the right type, such that the function DecodeEthernet in decode-ethernet.c is executed a second time. At this point, the algorithm cuts the first part of the packet and doesn't determine the current length. Specifically, if the packet is exactly 28 long, in the first iteration it subtracts 14 bytes. Then, it is working with a packet length of 14. At this point, the case distinction says it is a valid packet. After that it casts the packet, but this packet has no type, and the program crashes at the type case distinction.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4779
1385	CVE-2019-10055	HIGH	HIGH	An issue was discovered in Suricata 4.1.3. The function ftp_pasv_response lacks a check for the length of part1 and part2, leading to a crash within the ftp/mod.rs file.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4780
1386	CVE-2019-10054	MEDIUM	HIGH	An issue was discovered in Suricata 4.1.3. The function process_reply_record_v3 lacks a check for the length of reply.data. It causes an invalid memory access and the program crashes within the nfs/nfs3.rs file.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4781
1387	CVE-2019-10053	High	CRITICAL	An issue was discovered in Suricata 4.1.x before 4.1.4. If the input of the function SSHParseBanner is composed only of a \ n character, then the program runs into a heap-based buffer over-read. This occurs because the erroneous search for \r results in an integer underflow.	suricata	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4071
1388	CVE-2019-10051	MEDIUM	HIGH	An issue was discovered in Suricata 4.1.3. If the function filetracker_newchunk encounters an unsafe Some(sfcm) => { ft.new_chunk } item, then the program enters an smb/files.rs error condition and crashes.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4783
1389	CVE-2019-10050	Medium	HIGH	A buffer over-read issue was discovered in Suricata 4.1.x before 4.1.4. If the input of the decode-mpls.c function DecodeMPLS is composed only of a packet of source address and destination address plus the correct type field and the right number for shim, an attacker can manipulate the control flow, such that the condition to leave the loop is true. After leaving the loop, the network packet has a length of 2 bytes. There is no validation of this length. Later on, the code tries to read at an empty position, leading to a crash.	suricata	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4072
1390	CVE-2019-1002101	Medium	MEDIUM	The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Kubernetes creates a tar inside the container, copies it over the network, and kubectl unpacks it on the user?s machine. If the tar binary in the container is malicious, it could run any code and output unexpected, malicious results. An attacker could use this to write files to any path on the user?s machine when kubectl cp is called, limited only by the system permissions of the local user. The untar function can both create and follow symbolic links. The issue is resolved in kubectl v1.11.9, v1.12.7, v1.13.5, and v1.14.0.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3834
1391	CVE-2019-1002100	Medium	MEDIUM	In all Kubernetes versions prior to v1.11.8, v1.12.6, and v1.13.4, users that are authorized to make patch requests to the Kubernetes API Server can send a specially crafted patch of type json-patch (e.g. `kubectl patch --type json` or `Content-Type: application/json-patch+json`) that consumes excessive resources while processing, causing a Denial of Service on the API Server.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3835
1392	CVE-2019-1000020	Medium	MEDIUM	libarchive version commit 5a98dcf8a86364b3c2c469c85b93647dfb139961 onwards (version v2.8.0 onwards) contains a CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in ISO9660 parser, archive_read_support_format_iso9660.c, read_CE()/parse_rockridge() that can result in DoS by infinite loop. This attack appears to be exploitable via the victim opening a specially crafted ISO9660 file.	libarchive	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3560
1393	CVE-2019-1000019	Medium	MEDIUM	libarchive version commit bf9aec176c6748f0ee7a678c5f9f9555b9a757c1 onwards (release v3.0.2 onwards) contains a CWE-125: Out-of-bounds Read vulnerability in 7zip decompression, archive_read_support_format_7zip.c, header_bytes() that can result in a crash (denial of service). This attack appears to be exploitable via the victim opening a specially crafted 7zip file.	libarchive	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3531
1394	CVE-2019-1000016	Medium	MEDIUM	FFMPEG version 4.1 contains a CWE-129: Improper Validation of Array Index vulnerability in libavcodec/cbs_av1.c that can result in Denial of service. This attack appears to be exploitable via specially crafted AV1 file has to be provided as input. This vulnerability appears to have been fixed in after commit b97a4b658814b2de8b9f2a3bce491c002d34de31.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3499
1395	CVE-2019-0220	Medium	MEDIUM	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.	apache	Unchanged	Investigate	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4264
1396	CVE-2019-0217	Medium	HIGH	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3872
1397	CVE-2019-0215	Medium	HIGH	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3873

	A	B	C	D	E	F	G	H	I	J	K	L	M
1398	CVE-2019-0211	High	HIGH	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.	apache	Unchanged	Not vulnerable	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3874
1399	CVE-2019-0210	MEDIUM	HIGH	In Apache Thrift 0.9.3 to 0.12.0, a server implemented in Go using TJSONProtocol or TSimpleJSONProtocol may panic when feed with invalid input data.	thrift	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5178
1400	CVE-2019-0205	HIGH	HIGH	In Apache Thrift all versions up to and including 0.12.0, a server or client may run into an endless loop when feed with specific input data. Because the issue had already been partially fixed in version 0.11.0, depending on the installed version it affects only certain language bindings.	thrift	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5179
1401	CVE-2019-0203	Medium	HIGH	In Apache Subversion versions up to and including 1.9.10, 1.10.4, 1.12.0, Subversion's svnserve server process may exit when a client sends certain sequences of protocol commands. This can lead to disruption for users of the server.	subversion	Unchanged	Investigate	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5005
1402	CVE-2019-0197	Medium	MEDIUM	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set H2Upgrade on are unaffected by this issue.	apache	Unchanged	Not vulnerable	Not vulnerable	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4263
1403	CVE-2019-0196	Medium	MEDIUM	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.	apache	Unchanged	Not vulnerable	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4262
1404	CVE-2019-0190	MEDIUM	HIGH	A bug exists in the way mod_ssl handled client renegotiations. A remote attacker could send a carefully crafted request that would cause mod_ssl to enter a loop leading to a denial of service. This bug can be only triggered with Apache HTTP Server version 2.4.37 when using OpenSSL version 1.1.1 or later, due to an interaction in changes to handling of renegotiation attempts.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3528
1405	CVE-2019-0155	HIGH	HIGH	Insufficient access control in a subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6, E-2100 and E-2200 Processor Families; Intel(R) Graphics Driver for Windows before 26.20.100.6813 (DCH) or 26.20.100.6812 and before 21.20.x.5077 (aka15.45.5077), i915 Linux Driver for Intel(R) Processor Graphics before versions 5.4-rc7, 5.3.11, 4.19.84, 4.14.154, 4.9.201, 4.4.201 may allow an authenticated user to potentially enable escalation of privilege via local access.	linux	Unchanged	Not vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	LIN1019-3784
1406	CVE-2019-0154	LOW	MEDIUM	Insufficient access control in subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6 and E-2100 Processor Families may allow an authenticated user to potentially enable denial of service via local access.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	LIN1019-3783
1407	CVE-2019-0150	LOW	MEDIUM	Insufficient access control in firmware Intel(R) Ethernet 700 Series Controllers versions before 7.0 may allow a privileged user to potentially enable a denial of service via local access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3464
1408	CVE-2019-0149	LOW	MEDIUM	Insufficient input validation in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 2.8.43 may allow an authenticated user to potentially enable a denial of service via local access.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1019-3463
1409	CVE-2019-0148	LOW	MEDIUM	Resource leak in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 7.0 may allow an authenticated user to potentially enable a denial of service via local access.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1019-3462
1410	CVE-2019-0147	LOW	MEDIUM	Insufficient input validation in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 7.0 may allow an authenticated user to potentially enable a denial of service via local access.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1019-3461
1411	CVE-2019-0146	LOW	MEDIUM	Resource leak in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 2.8.43 may allow an authenticated user to potentially enable a denial of service via local access.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1019-3460
1412	CVE-2019-0145	HIGH	HIGH	Buffer overflow in i40e driver for Intel(R) Ethernet 700 Series Controllers versions before 7.0 may allow an authenticated user to potentially enable an escalation of privilege via local access.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1019-3456
1413	CVE-2019-0144	MEDIUM	MEDIUM	Unhandled exception in firmware for Intel(R) Ethernet 700 Series Controllers before version 7.0 may allow an authenticated user to potentially enable a denial of service via local access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.20.3.0	LIN1019-3459
1414	CVE-2019-0143	MEDIUM	MEDIUM	Unhandled exception in Kernel-mode drivers for Intel(R) Ethernet 700 Series Controllers versions before 7.0 may allow an authenticated user to potentially enable a denial of service via local access.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1019-3458

	A	B	C	D	E	F	G	H	I	J	K	L	M
1415	CVE-2019-0140	MEDIUM	HIGH	Buffer overflow in firmware for Intel(R) Ethernet 700 Series Controllers before version 7.0 may allow an unauthenticated user to potentially enable an escalation of privilege via an adjacent access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3454
1416	CVE-2019-0139	MEDIUM	MEDIUM	Insufficient access control in firmware for Intel(R) Ethernet 700 Series Controllers before version 7.0 may allow a privileged user to potentially enable an escalation of privilege, denial of service, or information disclosure via local access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3457
1417	CVE-2018-9996	MEDIUM	MEDIUM	An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_template_value_parm, demangle_integral_value, and demangle_expression.	binutils	Unchanged	8.0.0.27	Vulnerable	Vulnerable	Not vulnerable	Vulnerable	Vulnerable	LIN10-3730
1418	CVE-2018-9989	MEDIUM	HIGH	ARM mbed TLS before 2.1.11, before 2.7.2, and before 2.8.0 has a buffer over-read in ssl_parse_server_psk_hint() that could cause a crash on invalid input.	mbedtls	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3748
1419	CVE-2018-9988	MEDIUM	HIGH	ARM mbed TLS before 2.1.11, before 2.7.2, and before 2.8.0 has a buffer over-read in ssl_parse_server_key_exchange() that could cause a crash on invalid input.	mbedtls	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3735
1420	CVE-2018-9862	HIGH	HIGH	util.c in runV 1.0.0 for Docker mishandles a numeric username, which allows attackers to obtain root access by leveraging the presence of an initial numeric value on an /etc/passwd line, and then issuing a docker exec command with that value in the -u argument, a similar issue to CVE-2016-3697.	runv	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3741
1421	CVE-2018-9841	MEDIUM	HIGH	The export function in libavfilter/vf_signature.c in FFmpeg through 3.4.2 allows remote attackers to cause a denial of service (out-of-array access) or possibly have unspecified other impact via a long filename.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3739
1422	CVE-2018-9568	HIGH	HIGH	In sk_clone_lock of sock.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-113509306. References: Upstream kernel.	linux	Unchanged	8.0.0.31	9.0.0.22	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4332
1423	CVE-2018-9518	HIGH	HIGH	A flaw was found in the Linux kernel in nfc_llcp_build_sdreq_tlv() in net/nfc/llcp_commands.c that lack of size check may lead to an out of bounds write.	linux	Unchanged	8.0.0.29	9.0.0.20	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-5016
1424	CVE-2018-9517	HIGH	MEDIUM	A race condition between pppol2tp_session_create() and l2tp_eth_create() in net/l2tp/l2tp_netlink.c in the Linux kernel. Calling l2tp_tunnel_find() may result in a new tunnel being created with tunnel id of a previous removed tunnel which wouldn't be protected by the reference counter.	linux	Unchanged	8.0.0.29	9.0.0.20	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-5004
1425	CVE-2018-9516	HIGH	HIGH	In hid_debug_events_read of drivers/hid/hid-debug.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-71361580.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4333
1426	CVE-2018-9465	MEDIUM	HIGH	The Linux kernel is vulnerable to a use-after-free in drivers/android/binder.c. An attacker with local access could potentially exploit this to execute code.	linux	Unchanged	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4618
1427	CVE-2018-9422	HIGH	HIGH	A flaw was found in the way futex deals with the key handling for shared futexes. This allows a rare race condition that requires the page lock in the slow path when examining the swapcache.	linux	Unchanged	8.0.0.27	9.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4385
1428	CVE-2018-9363	HIGH	HIGH	A buffer overflow was found in hidp_process_report in hidp/core.c. The buffer length is unsigned at all layers, but gets cast to int and checked in hidp_process_report.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4635
1429	CVE-2018-9336	MEDIUM	HIGH	openvpnserv.exe (aka the interactive service helper) in OpenVPN 2.4.x before 2.4.6 allows a local attacker to cause a double-free of memory by sending a malformed request to the interactive service. This could cause a denial-of-service through memory corruption or possibly have unspecified other impact including privilege escalation.	openvpn	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3924
1430	CVE-2018-9274	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, ui/failure_message.c has a memory leak.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3723
1431	CVE-2018-9273	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-pcp.c has a memory leak.	wireshark	Unchanged	Not vulnerable	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3745
1432	CVE-2018-9272	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-h223.c has a memory leak.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3746
1433	CVE-2018-9271	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-multipart.c has a memory leak.	wireshark	Unchanged	Not vulnerable	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3752
1434	CVE-2018-9270	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/oids.c has a memory leak.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3759
1435	CVE-2018-9269	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-giop.c has a memory leak.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3747
1436	CVE-2018-9268	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-smb2.c has a memory leak.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3762
1437	CVE-2018-9267	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-lapd.c has a memory leak.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3729
1438	CVE-2018-9266	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-isup.c has a memory leak.	wireshark	Unchanged	Not vulnerable	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3742
1439	CVE-2018-9265	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, epan/dissectors/packet-tn3270.c has a memory leak.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3743
1440	CVE-2018-9264	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the ADB dissector could crash with a heap-based buffer overflow. This was addressed in epan/dissectors/packet-adb.c by checking for a length inconsistency.	wireshark	Unchanged	Not vulnerable	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3728

	A	B	C	D	E	F	G	H	I	J	K	L	M
1441	CVE-2018-9263	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the Kerberos dissector could crash. This was addressed in epan/dissectors/packet-kerberos.c by ensuring a nonzero key length.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3756
1442	CVE-2018-9262	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the VLAN dissector could crash. This was addressed in epan/dissectors/packet-vlan.c by limiting VLAN tag nesting to restrict the recursion depth.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3737
1443	CVE-2018-9261	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the NBAP dissector could crash with a large loop that ends with a heap-based buffer overflow. This was addressed in epan/dissectors/packet-nbap.c by prohibiting the self-linking of DCH-IDs.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3750
1444	CVE-2018-9260	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the IEEE 802.15.4 dissector could crash. This was addressed in epan/dissectors/packet-ieee802154.c by ensuring that an allocation step occurs.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3758
1445	CVE-2018-9259	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the MP4 dissector could crash. This was addressed in epan/dissectors/file-mp4.c by restricting the box recursion depth.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3722
1446	CVE-2018-9258	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5, the TCP dissector could crash. This was addressed in epan/dissectors/packet-tcp.c by preserving valid data sources.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3755
1447	CVE-2018-9257	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5, the CQL dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-cql.c by checking for a nonzero number of columns.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3733
1448	CVE-2018-9256	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.5 and 2.2.0 to 2.2.13, the LWAPP dissector could crash. This was addressed in epan/dissectors/packet-lwapp.c by limiting the encapsulation levels to restrict the recursion depth.	wireshark	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3726
1449	CVE-2018-9252	MEDIUM	MEDIUM	JasPer 2.0.14 allows denial of service via a reachable assertion in the function jpc_abstorelstepsize in libjasper/jpc/jpc_enc.c.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3753
1450	CVE-2018-9251	LOW	MEDIUM	The xz_decomp function in xzlib.c in libxml2 2.9.8, if --with-lzma is used, allows remote attackers to cause a denial of service (infinite loop) via a crafted XML file that triggers LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035.	libxml2	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-3736
1451	CVE-2018-9234	MEDIUM	HIGH	GnuPG 2.2.4 and 2.2.5 does not enforce a configuration in which key certification requires an offline master Certify key, which results in apparently valid certifications that occurred only with access to a signing subkey.	gnupg	Unchanged	Not vulnerable	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3725
1452	CVE-2018-9154	MEDIUM	HIGH	There is a reachable abort in the function jpc_dec_process_sot in libjasper/jpc/jpc_dec.c of JasPer 2.0.14 that will lead to a remote denial of service attack by triggering an unexpected jas_alloc2 return value, a different vulnerability than CVE-2017-13745.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3937
1453	CVE-2018-9138	MEDIUM	MEDIUM	An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.29 and 2.30. Stack Exhaustion occurs in the the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_nested_args, demangle_args, do_arg, and do_type.	binutils	Unchanged	8.0.0.27	Vulnerable	Vulnerable	Not vulnerable	10.19.45.1	Not vulnerable	LIN10-3653
1454	CVE-2018-9135	MEDIUM	HIGH	In ImageMagick 7.0.7-24 Q16, there is a heap-based buffer over-read in IsWEBPImageLossless in coders/webp.c.	imagemagick	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3630
1455	CVE-2018-9133	MEDIUM	MEDIUM	ImageMagick 7.0.7-26 Q16 has excessive iteration in the DecodeLabImage and EncodeLabImage functions (coders/tiff.c), which results in a hang (tens of minutes) with a tiny PoC file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted tiff file.	imagemagick	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3645
1456	CVE-2018-9055	Medium	MEDIUM	JasPer 2.0.14 allows denial of service via a reachable assertion in the function jpc_firstone in libjasper/jpc/jpc_math.c.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3636
1457	CVE-2018-8960	MEDIUM	HIGH	The ReadTIFFImage function in coders/tiff.c in ImageMagick 7.0.7-26 Q16 does not properly restrict memory allocation, leading to a heap-based buffer over-read.	imagemagick	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3632
1458	CVE-2018-8945	MEDIUM	MEDIUM	The bfd_section_from_shdr function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (segmentation fault) via a large attribute section.	binutils	Unchanged	8.0.0.27	9.0.0.20	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3637
1459	CVE-2018-8905	MEDIUM	HIGH	In LibTIFF 4.0.9, a heap-based buffer overflow occurs in the function LZWDecodeCompat in tif_lzw.c via a crafted TIFF file, as demonstrated by tiff2ps.	libtiff	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3631
1460	CVE-2018-8897	HIGH	HIGH	A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's Manual (SDM) was mishandled in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB exceptions that are deferred by MOV SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen configurations, or FreeBSD, or a Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpoints, and single step trap exceptions until the instruction boundary following the next instruction (SDM Vol. 3A; section 6.8.3). (The inhibited data breakpoints are those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions are not inhibited by the interrupt enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or POP to SS instruction is an instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, the debug exception is delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may therefore experience unexpected behavior when it occurs.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3888

	A	B	C	D	E	F	G	H	I	J	K	L	M
1461	CVE-2018-8883	MEDIUM	HIGH	Netwide Assembler (NASM) 2.13.02rc2 has a buffer over-read in the parse_line function in asm/parser.c via uncontrolled access to nasm_reg_flags.	nasm	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3656
1462	CVE-2018-8882	MEDIUM	HIGH	Netwide Assembler (NASM) 2.13.02rc2 has a stack-based buffer under-read in the function ieee_shr in asm/float.c via a large shift value.	nasm	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3664
1463	CVE-2018-8881	MEDIUM	HIGH	Netwide Assembler (NASM) 2.13.02rc2 has a heap-based buffer over-read in the function tokenize in asm/preproc.c, related to an unterminated string.	nasm	Unchanged	8.0.0.26	9.0.0.16	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3660
1464	CVE-2018-8822	HIGH	HIGH	Incorrect buffer length handling in the ncp_read_kernel function in fs/ncpfs/ncplib_kernel.c in the Linux kernel through 4.15.11, and in drivers/staging/ncpfs/ncplib_kernel.c in the Linux kernel 4.16-rc through 4.16-rc6, could be exploited by malicious NCPFS servers to crash the kernel or execute code.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3668
1465	CVE-2018-8804	MEDIUM	HIGH	WriteEPTImage in coders/ept.c in ImageMagick 7.0.7-25 Q16 allows remote attackers to cause a denial of service (MagickCore/memory.c double free and application crash) or possibly have unspecified other impact via a crafted file.	imagemagick	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3650
1466	CVE-2018-8789	HIGH	CRITICAL	FreeRDP prior to version 2.0.0-rc4 contains several Out-Of-Bounds Reads in the NTLM Authentication module that results in a Denial of Service (segfault).	freerdp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3241
1467	CVE-2018-8788	HIGH	CRITICAL	FreeRDP prior to version 2.0.0-rc4 contains an Out-Of-Bounds Write of up to 4 bytes in function nsc_rle_decode() that results in a memory corruption and possibly even a remote code execution.	freerdp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3234
1468	CVE-2018-8787	HIGH	CRITICAL	FreeRDP prior to version 2.0.0-rc4 contains an Integer Overflow that leads to a Heap-Based Buffer Overflow in function gdi_Bitmap_Decompress() and results in a memory corruption and probably even a remote code execution.	freerdp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3222
1469	CVE-2018-8786	HIGH	CRITICAL	FreeRDP prior to version 2.0.0-rc4 contains an Integer Truncation that leads to a Heap-Based Buffer Overflow in function update_read_bitmap_update() and results in a memory corruption and probably even a remote code execution.	freerdp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3218
1470	CVE-2018-8785	HIGH	CRITICAL	FreeRDP prior to version 2.0.0-rc4 contains a Heap-Based Buffer Overflow in function zgfx_decompress() that results in a memory corruption and probably even a remote code execution.	freerdp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3231
1471	CVE-2018-8784	HIGH	CRITICAL	FreeRDP prior to version 2.0.0-rc4 contains a Heap-Based Buffer Overflow in function zgfx_decompress_segment() that results in a memory corruption and probably even a remote code execution.	freerdp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3256
1472	CVE-2018-8781	HIGH	HIGH	The udl_fb_mmap function in drivers/gpu/drm/udl/udl_fb.c at the Linux kernel version 3.4 and up to and including 4.15 has an integer-overflow vulnerability allowing local users with access to the udldrmfb driver to obtain full read and write permissions on kernel physical pages, resulting in a code execution in kernel space.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3874
1473	CVE-2018-8780	HIGH	CRITICAL	In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, the Dir.open, Dir.new, Dir.entries and Dir.empty? methods do not check NULL characters. When using the corresponding method, unintentional directory traversal may be performed.	ruby	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3751
1474	CVE-2018-8779	MEDIUM	HIGH	In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, the UNIXServer.open and UNIXSocket.open methods are not checked for null characters. It may be connected to an unintended socket.	ruby	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3734
1475	CVE-2018-8778	MEDIUM	HIGH	In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, an attacker controlling the unpacking format (similar to format string vulnerabilities) can trigger a buffer under-read in the String#unpack method, resulting in a massive and controlled information disclosure.	ruby	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3757
1476	CVE-2018-8777	MEDIUM	HIGH	In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, an attacker can pass a large HTTP request with a crafted header to WEBrick server or a crafted body to WEBrick server/handler and cause a denial of service (memory consumption).	ruby	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3761
1477	CVE-2018-8769	MEDIUM	HIGH	elfutils 0.170 has a buffer over-read in the ebl_dynamic_tag_name function of libebl/ebldynamictagname.c because SYMTAB_SHNDX is unsupported.	elfutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3629
1478	CVE-2018-8740	MEDIUM	HIGH	In SQLite through 3.22.0, databases whose schema is corrupted using a CREATE TABLE AS statement could cause a NULL pointer dereference, related to build.c and prepare.c.	sqlite3	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4229
1479	CVE-2018-8736	HIGH	HIGH	A privilege escalation vulnerability in Nagios XI 5.2.x through 5.4.x before 5.4.13 allows an attacker to leverage an RCE vulnerability escalating to root.	nagios	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3842
1480	CVE-2018-8735	HIGH	HIGH	Remote command execution (RCE) vulnerability in Nagios XI 5.2.x through 5.4.x before 5.4.13 allows an attacker to execute arbitrary commands on the target system, aka OS command injection.	nagios	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3827
1481	CVE-2018-8734	HIGH	CRITICAL	SQL injection vulnerability in the core config manager in Nagios XI 5.2.x through 5.4.x before 5.4.13 allows an attacker to execute arbitrary SQL commands via the selInfoKey1 parameter.	nagios	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3813
1482	CVE-2018-8733	MEDIUM	HIGH	Authentication bypass vulnerability in the core config manager in Nagios XI 5.2.x through 5.4.x before 5.4.13 allows an unauthenticated attacker to make configuration changes and leverage an authenticated SQL injection vulnerability.	nagios	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3807
1483	CVE-2018-8099	MEDIUM	MEDIUM	Incorrect returning of an error code in the index.c:read_entry() function leads to a double free in libgit2 before v0.26.2, which allows an attacker to cause a denial of service via a crafted repository index file.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3560

	A	B	C	D	E	F	G	H	I	J	K	L	M
1484	CVE-2018-8098	MEDIUM	MEDIUM	Integer overflow in the index.c:read_entry() function while decompressing a compressed prefix length in libgit2 before v0.26.2 allows an attacker to cause a denial of service (out-of-bounds read) via a crafted repository index file.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3509
1485	CVE-2018-8087	MEDIUM	MEDIUM	Memory leak in the hwsim_new_radio_nl function in drivers/net/wireless/mac80211_hwsim.c in the Linux kernel through 4.15.9 allows local users to cause a denial of service (memory consumption) by triggering an out-of-array error case.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3581
1486	CVE-2018-8086			The basename implementation in string/basename.c in the GNU C Library (aka glibc or libc6) 2.26 allows attackers to cause a denial of service (segmentation fault), within the assembly code for strrchr, via a crafted argument.	glibc	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3582
1487	CVE-2018-8050	MEDIUM	MEDIUM	The af_get_page() function in lib/afflib_pages.cpp in AFFLIB (aka AFFLIBv3) through 3.7.16 allows remote attackers to cause a denial of service (segmentation fault) via a corrupt AFF image that triggers an unexpected pagesize value.	afflib	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3514
1488	CVE-2018-8043	LOW	MEDIUM	The unimac_mdio_probe function in drivers/net/phy/mdio-bcm-unimac.c in the Linux kernel through 4.15.8 does not validate certain resource availability, which allows local users to cause a denial of service (NULL pointer dereference).	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3546
1489	CVE-2018-8011	MEDIUM	HIGH	By specially crafting HTTP requests, the mod_md challenge handler would dereference a NULL pointer and cause the child process to segfault. This could be used to DoS the server. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.33).	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4367
1490	CVE-2018-7995	MEDIUM	MEDIUM	Race condition in the store_int_with_restart() function in arch/x86/kernel/cpu/mcheck/mce.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (panic) by leveraging root access to write to the check_interval file in a /sys/devices/system/machinecheck/machinecheck<cpu number> directory.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3556
1491	CVE-2018-7858	LOW	MEDIUM	Quick Emulator (aka QEMU), when built with the Cirrus CLGD 54xx VGA Emulator support, allows local guest OS privileged users to cause a denial of service (out-of-bounds access and QEMU process crash) by leveraging incorrect region calculation when updating VGA display.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3564
1492	CVE-2018-7757	LOW	MEDIUM	Memory leak in the sas_smp_get_phy_events function in drivers/scsi/libsas/sas_expander.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (memory consumption) via many read accesses to files in the /sys/class/sas_phy directory, as demonstrated by the /sys/class/sas_phy/phy-1:0:12/invalid_dword_count file.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3571
1493	CVE-2018-7755	LOW	MEDIUM	An issue was discovered in the fd_locked_ioctl function in drivers/block/floppy.c in the Linux kernel through 4.15.7. The floppy driver will copy a kernel pointer to user memory in response to the FDGETPRM ioctl. An attacker can send the FDGETPRM ioctl and use the obtained kernel pointer to discover the location of kernel code and data and bypass kernel security protections such as KASLR.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3568
1494	CVE-2018-7754	LOW	MEDIUM	The aoedisk_debugfs_show function in drivers/block/aoe/aoeblk.c in the Linux kernel through 4.16.4rc4 allows local users to obtain sensitive address information by reading ffree: lines in a debugfs file.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4539
1495	CVE-2018-7751	MEDIUM	MEDIUM	The svg_probe function in libavformat/img2dec.c in FFmpeg through 3.4.2 allows remote attackers to cause a denial of service (Infinite Loop) via a crafted XML file.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3868
1496	CVE-2018-7740	MEDIUM	MEDIUM	The resv_map_release function in mm/hugetlb.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (BUG) via a crafted application that makes mmap system calls and has a large pgoff argument to the remap_file_pages system call.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3558
1497	CVE-2018-7738	HIGH	HIGH	In util-linux before 2.32-rc1, bash-completion/umount allows local users to gain privileges by embedding shell commands in a mountpoint name, which is mishandled during a umount command (within Bash) by a different user, as demonstrated by logging in as root and entering umount followed by a tab character for autocompletion.	until-linux	Unchanged	Not vulnerable	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3523
1498	CVE-2018-7714	MEDIUM	HIGH	The validateInputImageSize function in modules/imgcodecs/src/loadsave.cpp in OpenCV 3.4.1 allows remote attackers to cause a denial of service (assertion failure) because (pixels <= (1<<30)) may be false.	opencv	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3533
1499	CVE-2018-7713	MEDIUM	HIGH	The validateInputImageSize function in modules/imgcodecs/src/loadsave.cpp in OpenCV 3.4.1 allows remote attackers to cause a denial of service (assertion failure) because (size.width <= (1<<20)) may be false.	opencv	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3575
1500	CVE-2018-7712	MEDIUM	HIGH	The validateInputImageSize function in modules/imgcodecs/src/loadsave.cpp in OpenCV 3.4.1 allows remote attackers to cause a denial of service (assertion failure) because (size.height <= (1<<20)) may be false.	opencv	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3513
1501	CVE-2018-7648	HIGH	CRITICAL	An issue was discovered in mj2/opj_mj2_extract.c in OpenJPEG 2.3.0. The output prefix was not checked for length, which could overflow a buffer, when providing a prefix with 50 or more characters on the command line.	openjpeg	Unchanged	Won't Fix	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3565
1502	CVE-2018-7643	MEDIUM	HIGH	The display_debug_ranges function in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, as demonstrated by objdump.	binutils	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3570

	A	B	C	D	E	F	G	H	I	J	K	L	M
1503	CVE-2018-7642	MEDIUM	MEDIUM	The swap_std_reloc_in function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (aout_32_swap_std_reloc_out NULL pointer dereference and application crash) via a crafted ELF file, as demonstrated by objcopy.	binutils	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3530
1504	CVE-2018-7584	HIGH	CRITICAL	In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.	php	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3553
1505	CVE-2018-7570	MEDIUM	MEDIUM	The assign_file_positions_for_non_load_sections function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an ELF file with a RELRO segment that lacks a matching LOAD segment, as demonstrated by objcopy.	binutils	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3548
1506	CVE-2018-7569	MEDIUM	MEDIUM	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer underflow or overflow, and application crash) via an ELF file with a corrupt DWARF FORM block, as demonstrated by nm.	binutils	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3528
1507	CVE-2018-7568	MEDIUM	MEDIUM	The parse_die function in dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer overflow and application crash) via an ELF file with corrupt dwarf1 debug information, as demonstrated by nm.	binutils	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3521
1508	CVE-2018-7566	MEDIUM	HIGH	The Linux kernel 4.15 has a Buffer Overflow via an SNDRV_SEQ_IOCTL_SET_CLIENT_POOL ioctl write operation to /dev/snd/seq by a local user.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3635
1509	CVE-2018-7557	MEDIUM	MEDIUM	The decode_init function in libavcodec/utvideodec.c in FFmpeg through 3.4.2 allows remote attackers to cause a denial of service (Out of array read) via an AVI file with crafted dimensions within chroma subsampling data.	ffmpeg	Unchanged	Won't Fix	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3544
1510	CVE-2018-7550	MEDIUM	HIGH	The load_multiboot function in hw/i386/multiboot.c in Quick Emulator (aka QEMU) allows local guest OS users to execute arbitrary code on the QEMU host via a mh_load_end_addr value greater than mh_bss_end_addr, which triggers an out-of-bounds read or write memory access.	qemu	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3550
1511	CVE-2018-7549	MEDIUM	HIGH	In params.c in zsh through 5.4.2, there is a crash during a copy of an empty hash table, as demonstrated by typeset -p.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3543
1512	CVE-2018-7548	HIGH	CRITICAL	In subst.c in zsh through 5.4.2, there is a NULL pointer dereference when using ${(PA)...} on an empty array result.	zsh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-3508
1513	CVE-2018-7544	MEDIUM	CRITICAL	** DISPUTED ** A cross-protocol scripting issue was discovered in the management interface in OpenVPN through 2.4.5. When this interface is enabled over TCP without a password, and when no other clients are connected to this interface, attackers can execute arbitrary management commands, obtain sensitive information, or cause a denial of service (SIGTERM) by triggering XMLHttpRequest actions in a web browser. This is demonstrated by a multipart/form-data POST to http://localhost:23000 with a signal SIGTERM command in a TEXTAREA element. NOTE: The vendor disputes that this is a vulnerability. They state that this is the result of improper configuration of the OpenVPN instance rather than an intrinsic vulnerability, and now more explicitly warn against such configurations in both the management-interface documentation, and with a runtime warning.	openvpn	Unchanged	Investigate	Investigate	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3678
1514	CVE-2018-7492	MEDIUM	MEDIUM	A NULL pointer dereference was found in the net/rds/rdma.c __rds_rdma_map() function in the Linux kernel before 4.14.7 allowing local attackers to cause a system panic and a denial-of-service, related to RDS_GET_MR and RDS_GET_MR_FOR_DEST.	linux	Unchanged	8.0.0.26	9.0.0.15	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3388
1515	CVE-2018-7490	MEDIUM	HIGH	uWSGI before 2.0.17 mishandles a DOCUMENT_ROOT check during use of the --php-docroot option, allowing directory traversal.	uwsgi	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3393
1516	CVE-2018-7485	HIGH	CRITICAL	The SQLWriteFileDSN function in odbcinst/SQLWriteFileDSN.c in unixODBC 2.3.5 has strncpy arguments in the wrong order, which allows attackers to cause a denial of service or possibly have unspecified other impact.	unixodbc	Unchanged	Not vulnerable	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3316
1517	CVE-2018-7480	HIGH	HIGH	The blkcg_init_queue function in block/blk-cgroup.c in the Linux kernel before 4.11 allows local users to cause a denial of service (double free) or possibly have unspecified other impact by triggering a creation failure.	linux	Unchanged	Not vulnerable	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3401
1518	CVE-2018-7470	MEDIUM	MEDIUM	An issue was discovered in ImageMagick 7.0.7-22 Q16. The IsWEBPImageLossless function in coders/webp.c allows attackers to cause a denial of service (segmentation violation) via a crafted file.	imagemagick	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3337
1519	CVE-2018-7456	MEDIUM	MEDIUM	A NULL Pointer Dereference occurs in the function TIFFPrintDirectory in tif_print.c in LibTIFF 4.0.9 when using the tiffinfo tool to print crafted TIFF information, a different vulnerability than CVE-2017-18013. (This affects an earlier part of the TIFFPrintDirectory function that was not addressed by the CVE-2017-18013 patch.)	libtiff	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3332
1520	CVE-2018-7443	MEDIUM	MEDIUM	The ReadTIFFImage function in coders/tiff.c in ImageMagick 7.0.7-23 Q16 does not properly validate the amount of image data in a file, which allows remote attackers to cause a denial of service (memory allocation failure in the AcquireMagickMemory function in MagickCore/memory.c).	imagemagick	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3430

	A	B	C	D	E	F	G	H	I	J	K	L	M
1521	CVE-2018-7442	MEDIUM	CRITICAL	An issue was discovered in Leptonica through 1.75.3. The gplotMakeOutput function does not block '/' characters in the gplot rootname argument, potentially leading to path traversal and arbitrary file overwrite.	leptonica	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3416
1522	CVE-2018-7441	MEDIUM	HIGH	Leptonica through 1.75.3 uses hardcoded /tmp pathnames, which might allow local users to overwrite arbitrary files or have unspecified other impact by creating files in advance or winning a race condition, as demonstrated by /tmp/junk_split_image.ps in prog/splitimage2pdf.c.	leptonica	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3357
1523	CVE-2018-7440	HIGH	CRITICAL	An issue was discovered in Leptonica through 1.75.3. The gplotMakeOutput function allows command injection via a $ (command) approach in the gplot rootname argument. This issue exists because of an incomplete fix for CVE-2018-3836.	leptonica	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3404
1524	CVE-2018-7421	MEDIUM	HIGH	In Wireshark 2.2.0 to 2.2.12 and 2.4.0 to 2.4.4, the DMP dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-dmp.c by correctly supporting a bounded number of Security Categories for a DMP Security Classification.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3377
1525	CVE-2018-7420	MEDIUM	HIGH	In Wireshark 2.2.0 to 2.2.12 and 2.4.0 to 2.4.4, the pcapng file parser could crash. This was addressed in wiretap/pcapng.c by adding a block-size check for sysdig event blocks.	wireshark	Unchanged	8.0.0.28	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3329
1526	CVE-2018-7419	MEDIUM	HIGH	In Wireshark 2.2.0 to 2.2.12 and 2.4.0 to 2.4.4, the NBAP dissector could crash. This was addressed in epan/dissectors/asn1/nbap/nbap.cnf by ensuring DCH ID initialization.	wireshark	Unchanged	Not vulnerable	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3367
1527	CVE-2018-7418	MEDIUM	HIGH	In Wireshark 2.2.0 to 2.2.12 and 2.4.0 to 2.4.4, the SIGCOMP dissector could crash. This was addressed in epan/dissectors/packet-sigcomp.c by correcting the extraction of the length value.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3319
1528	CVE-2018-7417	MEDIUM	HIGH	In Wireshark 2.2.0 to 2.2.12 and 2.4.0 to 2.4.4, the IPMI dissector could crash. This was addressed in epan/dissectors/packet-ipmi-picmg.c by adding support for crafted packets that lack an IPMI header.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3391
1529	CVE-2018-7409	HIGH	CRITICAL	In unixODBC before 2.3.5, there is a buffer overflow in the unicode_to_ansi_copy() function in DriverManager/__info.c.	unixodbc	Unchanged	Vulnerable	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3313
1530	CVE-2018-7337	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4, the DOCSIS protocol dissector could crash. This was addressed in plugins/docsis/packet-docsis.c by removing the recursive algorithm that had been used for concatenated PDUs.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3382
1531	CVE-2018-7336	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, the FCP protocol dissector could crash. This was addressed in epan/dissectors/packet-fcp.c by checking for a NULL pointer.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3429
1532	CVE-2018-7335	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, the IEEE 802.11 dissector could crash. This was addressed in epan/crypt/airpdcap.c by rejecting lengths that are too small.	wireshark	Unchanged	Not vulnerable	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3346
1533	CVE-2018-7334	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, the UMTS MAC dissector could crash. This was addressed in epan/dissectors/packet-umts_mac.c by rejecting a certain reserved value.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3342
1534	CVE-2018-7333	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-rpcrdma.c had an infinite loop that was addressed by validating a chunk size.	wireshark	Unchanged	Not vulnerable	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3390
1535	CVE-2018-7332	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-reload.c had an infinite loop that was addressed by validating a length.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3433
1536	CVE-2018-7331	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-ber.c had an infinite loop that was addressed by validating a length.	wireshark	Unchanged	8.0.0.28	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3363
1537	CVE-2018-7330	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-thread.c had an infinite loop that was addressed by using a correct integer data type.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3387
1538	CVE-2018-7329	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-s7comm.c had an infinite loop that was addressed by correcting off-by-one errors.	wireshark	Unchanged	Not vulnerable	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3386
1539	CVE-2018-7328	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-usb.c had an infinite loop that was addressed by rejecting short frame header lengths.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3371
1540	CVE-2018-7327	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-openflow_v6.c had an infinite loop that was addressed by validating property lengths.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3340
1541	CVE-2018-7326	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-lltd.c had an infinite loop that was addressed by using a correct integer data type.	wireshark	Unchanged	Not vulnerable	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3372
1542	CVE-2018-7325	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-rpki-rtr.c had an infinite loop that was addressed by validating a length field.	wireshark	Unchanged	Not vulnerable	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3405
1543	CVE-2018-7324	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-sccp.c had an infinite loop that was addressed by using a correct integer data type.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3380
1544	CVE-2018-7323	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-wccp.c had a large loop that was addressed by ensuring that a calculated length was monotonically increasing.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3358
1545	CVE-2018-7322	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-dcm.c had an infinite loop that was addressed by checking for integer wraparound.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3412
1546	CVE-2018-7321	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, epan/dissectors/packet-thrift.c had a large loop that was addressed by not proceeding with dissection after encountering an unexpected type.	wireshark	Unchanged	Not vulnerable	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3431
1547	CVE-2018-7320	MEDIUM	HIGH	In Wireshark 2.4.0 to 2.4.4 and 2.2.0 to 2.2.12, the SIGCOMP protocol dissector could crash. This was addressed in epan/dissectors/packet-sigcomp.c by validating operand offsets.	wireshark	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3400

	A	B	C	D	E	F	G	H	I	J	K	L	M
1548	CVE-2018-7273	MEDIUM	MEDIUM	In the Linux kernel through 4.15.4, the floppy driver reveals the addresses of kernel functions and global variables using printk calls within the function show_floppy in drivers/block/floppy.c. An attacker can read this information from dmesg and use the addresses to find the locations of kernel code and data and bypass kernel security protections such as KASLR.	linux	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3392
1549	CVE-2018-7263	MEDIUM	CRITICAL	The mad_decoder_run() function in decoder.c in Underbit libmad through 0.15.1b allows remote attackers to cause a denial of service (SIGABRT because of double free or corruption) or possibly have unspecified other impact via a crafted file. NOTE: this may overlap CVE-2017-11552.	libmad	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3356
1550	CVE-2018-7262	MEDIUM	HIGH	In Ceph before 12.2.3 and 13.x through 13.0.1, the rgw_civetweb.cc RGWCivetWeb::init_env function in radosgw doesn't handle malformed HTTP headers properly, allowing for denial of service.	ceph	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3667
1551	CVE-2018-7260	LOW	MEDIUM	Cross-site scripting (XSS) vulnerability in db_central_columns.php in phpMyAdmin before 4.7.8 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL.	phpmyadmin	Unchanged	Not vulnerable	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3369
1552	CVE-2018-7254	MEDIUM	HIGH	The ParseCaffHeaderConfig function of the cli/caff.c file of WavPack 5.1.0 allows a remote attacker to cause a denial-of-service (global buffer over-read), or possibly trigger a buffer overflow or incorrect memory allocation, via a maliciously crafted CAF file.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3428
1553	CVE-2018-7253	MEDIUM	HIGH	The ParseDsdiffHeaderConfig function of the cli/dsdiff.c file of WavPack 5.1.0 allows a remote attacker to cause a denial-of-service (heap-based buffer over-read) or possibly overwrite the heap via a maliciously crafted DSDIFF file.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3351
1554	CVE-2018-7247	HIGH	CRITICAL	An issue was discovered in pixHtmlViewer in prog/htmlviewer.c in Leptonica before 1.75.3. Unsanitized input (rootname) can overflow a buffer, leading potentially to arbitrary code execution or possibly unspecified other impact.	leptonica	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3325
1555	CVE-2018-7226	HIGH	CRITICAL	An issue was discovered in vcSetXCutTextProc() in VNConsole.c in LinuxVNC and VNCommand from the LibVNC/vncterm distribution through 0.9.10. Missing sanitization of the client-specified message length may cause integer overflow or possibly have unspecified other impact via a specially crafted VNC packet.	libvnc	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3336
1556	CVE-2018-7225	HIGH	CRITICAL	An issue was discovered in LibVNCServer through 0.9.11. rfbProcessClientNormalMessage() in rfbserver.c does not sanitize msg.cct.length, leading to access to uninitialized and potentially sensitive data or possibly unspecified other impact (e.g., an integer overflow) via specially crafted VNC packets.	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3410
1557	CVE-2018-7208	MEDIUM	HIGH	In the coff_pointerize_aux function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, an index is not validated, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted file, as demonstrated by objcopy of a COFF object.	binutils	Unchanged	8.0.0.26	9.0.0.15	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3324
1558	CVE-2018-7191	Medium	MEDIUM	In the tun subsystem in the Linux kernel before 4.13.14, dev_get_valid_name is not called before register_netdevice. This allows local users to cause a denial of service (NULL pointer dereference and panic) via an ioctl(TUNSETIFF) call with a dev name containing a / character. This is similar to CVE-2013-4343.	linux	Unchanged	8.0.0.31	9.0.0.22	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4093
1559	CVE-2018-7187	HIGH	HIGH	The go get implementation in Go 1.9.4, when the -insecure command-line option is used, does not validate the import path (get/vcs.go only checks for :// anywhere in the string), which allows remote attackers to execute arbitrary OS commands via a crafted web site.	go	Unchanged	Investigate	Won't Fix	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3418
1560	CVE-2018-7186	HIGH	CRITICAL	Leptonica before 1.75.3 does not limit the number of characters in a %s format argument to fscanf or sscanf, which allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a long string, as demonstrated by the gplotRead and ptaReadStream functions.	leptonica	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3427
1561	CVE-2018-7185	Medium	Low	The NTP Protocol allows for both non-authenticated and authenticated associations, in client/server, symmetric (peer), and several broadcast modes. In addition to the basic NTP operational modes, symmetric mode and broadcast servers can support an interleaved mode of operation. In ntp-4.2.8p4 a bug was inadvertently introduced into the protocol engine that allows a non- uthenticated zero-origin (reset) packet to reset an authenticated interleaved peer association. If an attacker can send a packet with a zero-origin timestamp and the source IP address of the "other side" of an interleaved association, the 'victim' ntpd will reset its association. The attacker must continue sending these packets in order to maintain the disruption of the association. In ntp-4.0.0 thru ntp-4.2.8p6, interleave mode could be entered dynamically. As of ntp-4.2.8p7, interleaved mode must be explicitly configured/enabled.	ntp	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3339
1562	CVE-2018-7184	Medium	Low	The fix for NtpBug2952 was incomplete, and while it fixed one problem it created another. Specifically, it drops bad packets before updating the "received" timestamp. This means a third-party can inject a packet with a zero-origin timestamp, meaning the sender wants to reset the association, and the transmit timestamp in this bogus packet will be saved as the most recent "received" timestamp. The real remote peer does not know this value and this will disrupt the association until the association resets.	ntp	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3411

	A	B	C	D	E	F	G	H	I	J	K	L	M
1563	CVE-2018-7183	Medium	Medium	ntpq is a monitoring and control program for ntpd. decodearr() is an internal function of ntpq that is used to -- wait for it -- decode an array in a response string when formatted data is being displayed. This is a problem in affected versions of ntpq if a maliciously-altered ntpd returns an array result that will trip this bug, or if a bad actor is able to read an ntpq request on its way to a remote ntpd server and forge and send a response before the remote ntpd sends its response. It's potentially possible that the malicious data could become injectable/executable code.	ntp	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3437
1564	CVE-2018-7182	Medium	Medium	ctl_getitem() is used by ntpd to process incoming mode 6 packets. A malicious mode 6 packet can be sent to an ntpd instance, and if the ntpd instance is from 4.2.8p6 thru 4.2.8p10, that will cause ctl_getitem() to read past the end of its buffer. displayed. This is a problem in affected versions of ntpq if a maliciously-altered ntpd returns an array result that will trip this bug, or if a bad actor is able to read an ntpq request on its way to a remote ntpd server and forge and send a response before the remote ntpd sends its response. It's potentially possible that the malicious data could become injectable/executable code.	ntp	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3417
1565	CVE-2018-7170	Low	Low	ntpd can be vulnerable to Sybil attacks. If a system is set up to use a trustedkey and if one is not using the feature introduced in ntp-4.2.8p6 allowing an optional 4th field in the ntp.keys file to specify which IPs can serve time, a malicious authenticated peer -- i.e. one where the attacker knows the private symmetric key -- can create arbitrarily-many ephemeral associations in order to win the clock selection of ntpd and modify a victim's clock. Three additional protections are offered in ntp-4.2.8p11. One is the new noepeer directive, which disables symmetric passive ephemeral peering. Another is the new ippeerlimit directive, which limits the number of peers that can be created from an IP. The third extends the functionality of the 4th field in the ntp.keys file to include specifying a subnet range.	ntp	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3399
1566	CVE-2018-7169	MEDIUM	MEDIUM	An issue was discovered in shadow 4.5. newgidmap (in shadow-utils) is setuid and allows an unprivileged user to be placed in a user namespace where setgroups(2) is permitted. This allows an attacker to remove themselves from a supplementary group, which may allow access to certain filesystem paths if the administrator has used group blacklisting (e.g., chmod g-rwx) to restrict access to paths. This flaw effectively reverts a security feature in the kernel (in particular, the /proc/self/setgroups knob) to prevent this sort of privilege escalation.	shadow	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3341
1567	CVE-2018-7160	MEDIUM	HIGH	The Node.js inspector, in 6.x and later is vulnerable to a DNS rebinding attack which could be exploited to perform remote code execution. An attack is possible from malicious websites open in a web browser on the same computer, or another computer with network access to the computer running the Node.js process. A malicious website could use a DNS rebinding attack to trick the web browser to bypass same-origin-policy checks and to allow HTTP connections to localhost or to hosts on the local network. If a Node.js process with the debug port active is running on localhost or on a host on the local network, the malicious website could connect to it as a debugger, and get full code execution access.	nodejs	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4030
1568	CVE-2018-7159	MEDIUM	MEDIUM	The HTTP parser in all current versions of Node.js ignores spaces in the `Content-Length` header, allowing input such as `Content-Length: 1 2` to be interpreted as having a value of `12`. The HTTP specification does not allow for spaces in the `Content-Length` value and the Node.js HTTP parser has been brought into line on this particular difference. The security risk of this flaw to Node.js users is considered to be VERY LOW as it is difficult, and may be impossible, to craft an attack that makes use of this flaw in a way that could not already be achieved by supplying an incorrect value for `Content-Length`. Vulnerabilities may exist in user-code that make incorrect assumptions about the potential accuracy of this value compared to the actual length of the data supplied. Node.js users crafting lower-level HTTP utilities are advised to re-check the length of any input supplied after parsing is complete.	nodejs	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4042
1569	CVE-2018-7158	MEDIUM	HIGH	The ``path`` module in the Node.js 4.x release line contains a potential regular expression denial of service (ReDoS) vector. The code in question was replaced in Node.js 6.x and later so this vulnerability only impacts all versions of Node.js 4.x. The regular expression, `splitPathRe`, used within the ``path`` module for the various path parsing functions, including `path.dirname()`, `path.extname()` and `path.parse()` was structured in such a way as to allow an attacker to craft a string, that when passed through one of these functions, could take a significant amount of time to evaluate, potentially leading to a full denial of service.	nodejs	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4046
1570	CVE-2018-7054	High	Critical	An issue was discovered in Irssi before 1.0.7 and 1.1.x before 1.1.1. There is a use-after-free when a server is disconnected during netsplits. NOTE: this issue exists because of an incomplete fix for CVE-2017-7191.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3389
1571	CVE-2018-7053	High	Critical	An issue was discovered in Irssi before 1.0.7 and 1.1.x before 1.1.1. There is a use-after-free when SASL messages are received in an unexpected order.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3310
1572	CVE-2018-7052	Medium	High	An issue was discovered in Irssi before 1.0.7 and 1.1.x before 1.1.1. When the number of windows exceeds the available space, a crash due to a NULL pointer dereference would occur.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3354

	A	B	C	D	E	F	G	H	I	J	K	L	M
1573	CVE-2018-7051	Medium	High	An issue was discovered in Irssi before 1.0.7 and 1.1.x before 1.1.1. Certain nick names could result in out-of-bounds access when printing theme strings.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3327
1574	CVE-2018-7050	Medium	High	An issue was discovered in Irssi before 1.0.7 and 1.1.x before 1.1.1. A NULL pointer dereference occurs for an empty nick.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3320
1575	CVE-2018-6954	HIGH	HIGH	systemd-tmpfiles in systemd through 237 mishandles symlinks present in non-terminal path components, which allows local users to obtain ownership of arbitrary files via vectors involving creation of a directory and a file under that directory, and later replacing that directory with a symlink. This occurs even if the fs.protected_symlinks sysctl is turned on.	systemd	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3419
1576	CVE-2018-6952	MEDIUM	HIGH	A double free exists in the another_hunk function in pch.c in GNU patch through 2.7.6.	patch	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3425
1577	CVE-2018-6951	MEDIUM	HIGH	An issue was discovered in GNU patch through 2.7.6. There is a segmentation fault, associated with a NULL pointer dereference, leading to a denial of service in the intuit_diff_type function in pch.c, aka a mangled rename issue.	patch	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3352
1578	CVE-2018-6942	MEDIUM	MEDIUM	An issue was discovered in FreeType 2 through 2.9. A NULL pointer dereference in the Ins_GETVARIATION() function within ttinterp.c could lead to DoS via a crafted font file.	freetype	Unchanged	Not vulnerable	Not vulnerable	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3432
1579	CVE-2018-6927	MEDIUM	HIGH	The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact by triggering a negative wake or requeue value.	linux	Unchanged	8.0.0.26	9.0.0.15	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3321
1580	CVE-2018-6913	HIGH	CRITICAL	Heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.	perl	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3862
1581	CVE-2018-6912	MEDIUM	MEDIUM	The decode_plane function in libavcodec/utvideodec.c in FFmpeg through 3.4.2 allows remote attackers to cause a denial of service (out of array read) via a crafted AVI file.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3421
1582	CVE-2018-6872	MEDIUM	MEDIUM	The elf_parse_notes function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (out-of-bounds read and segmentation violation) via a note with a large alignment.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3406
1583	CVE-2018-6836	HIGH	CRITICAL	The netmonrec_comment_destroy function in wiretap/netmon.c in Wireshark through 2.4.4 performs a free operation on an uninitialized memory address, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3331
1584	CVE-2018-6829	MEDIUM	HIGH	cipher/elgamal.c in Libgcrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintexts, which allows attackers to obtain sensitive information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). The Decisional Diffie-Hellman (DDH) assumption does not hold for Libgcrypt's ElGamal implementation.	libgcrypt	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN10-3323
1585	CVE-2018-6798	MEDIUM	HIGH	An issue was discovered in Perl 5.22 through 5.26. Matching a crafted locale dependent regular expression can cause a heap-based buffer over-read and potentially information disclosure.	perl	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3836
1586	CVE-2018-6797	HIGH	CRITICAL	An issue was discovered in Perl 5.18 through 5.26. A crafted regular expression can cause a heap-based buffer overflow, with control over the bytes written.	perl	Unchanged	8.0.0.27	9.0.0.17	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3853
1587	CVE-2018-6794	MEDIUM	MEDIUM	Suricata before 4.1 is prone to an HTTP detection bypass vulnerability in detect.c and stream-tcp.c. If a malicious server breaks a normal TCP flow and sends data before the 3-way handshake is complete, then the data sent by the malicious server will be accepted by web clients such as a web browser or Linux CLI utilities, but ignored by Suricata IDS signatures. This mostly affects IDS signatures for the HTTP protocol and TCP stream content; signatures for TCP packets will inspect such network traffic as usual.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3398
1588	CVE-2018-6767	MEDIUM	HIGH	A stack-based buffer over-read in the ParseRiffHeaderConfig function of cli/riff.c file of WavPack 5.1.0 allows a remote attacker to cause a denial-of-service attack or possibly have unspecified other impact via a maliciously crafted RF64 file.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3402
1589	CVE-2018-6764	MEDIUM	HIGH	util/virlog.c in libvirt does not properly determine the hostname on LXC container startup, which allows local guest OS users to bypass an intended container protection mechanism and execute arbitrary commands via a crafted NSS module.	libvirt	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3395
1590	CVE-2018-6759	MEDIUM	MEDIUM	The bfd_get_debug_link_info_1 function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, has an unchecked strnlen operation. Remote attackers could leverage this vulnerability to cause a denial of service (segmentation fault) via a crafted ELF file.	binutils	Unchanged	8.0.0.26	9.0.0.15	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3353
1591	CVE-2018-6621	MEDIUM	MEDIUM	The decode_frame function in libavcodec/utvideodec.c in FFmpeg through 3.4.1 allows remote attackers to cause a denial of service (out of array read) via a crafted AVI file.	ffmpeg	Unchanged	Not vulnerable	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3409
1592	CVE-2018-6616	MEDIUM	MEDIUM	In OpenJPEG 2.3.0, there is excessive iteration in the opj_t1_encode_cblks function of openjp2/t1.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.	openjpeg	Unchanged	Won't Fix	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3375
1593	CVE-2018-6594	MEDIUM	HIGH	lib/Crypto/PublicKey/ElGamal.py in PyCrypto through 2.6.1 generates weak ElGamal key parameters, which allows attackers to obtain sensitive information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). The Decisional Diffie-Hellman (DDH) assumption does not hold for PyCrypto's ElGamal implementation.	python-pycrypto	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3408

	A	B	C	D	E	F	G	H	I	J	K	L	M
1594	CVE-2018-6574	HIGH	CRITICAL	Go before 1.8.7, Go 1.9.x before 1.9.4, and Go 1.10 pre-releases before Go 1.10rc2 allow go get remote command execution during source code build, by leveraging the gcc or clang plugin feature, because -fplugin= and -plugin= arguments were not blocked.	go	Unchanged	Investigate	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3396
1595	CVE-2018-6559	LOW	LOW	The Linux kernel, as used in Ubuntu 18.04 LTS and Ubuntu 18.10, allows local users to obtain names of files in which they would not normally be able to access via an overlayfs mount inside of a user namespace.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4872
1596	CVE-2018-6557	MEDIUM	HIGH	The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu2.2, and Ubuntu 18.10 before 10.1ubuntu6 incorrectly handled temporary files. A local attacker could use this issue to cause a denial of service, or possibly escalate privileges if kernel symlink restrictions were disabled.	base-files	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4597
1597	CVE-2018-6555	HIGH	HIGH	The irda_setsockopt function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (ias_object use-after-free and system crash) or possibly have unspecified other impact via an AF_IRDA socket.	linux	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4682
1598	CVE-2018-6554	MEDIUM	MEDIUM	Memory leak in the irda_bind function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (memory consumption) by repeatedly binding an AF_IRDA socket.	linux	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4701
1599	CVE-2018-6553	MEDIUM	HIGH	The CUPS AppArmor profile incorrectly confined the dnssd backend due to use of hard links. A local attacker could possibly use this issue to escape confinement. This flaw affects versions prior to 2.2.7-1ubuntu2.1 in Ubuntu 18.04 LTS, prior to 2.2.4-7ubuntu3.1 in Ubuntu 17.10, prior to 2.1.3-4ubuntu0.5 in Ubuntu 16.04 LTS, and prior to 1.7.2-0ubuntu1.10 in Ubuntu 14.04 LTS.	cups	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4533
1600	CVE-2018-6551	High	Critical	The malloc implementation in the GNU C Library (aka glibc or libc6), from version 2.24 to 2.26 on powerpc, and only in version 2.26 on i386, did not properly handle malloc calls with arguments close to SIZE_MAX and could return a pointer to a heap region that is smaller than requested, eventually leading to heap corruption.	glibc	Unchanged	8.0.0.26	9.0.0.15	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3348
1601	CVE-2018-6543	Medium	High	In GNU Binutils 2.30, there's an integer overflow in the function load_specific_debug_section() in objdump.c, which results in `malloc()` with 0 size. A crafted ELF file allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.	binutils	Unchanged	8.0.0.26	9.0.0.15	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3394
1602	CVE-2018-6485	High	Critical	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.	glibc	Unchanged	8.0.0.26	9.0.0.15	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3330
1603	CVE-2018-6459	MEDIUM	MEDIUM	The rsa_pss_params_parse function in libstrongswan/credentials/keys/signature_params.c in strongSwan 5.6.1 allows remote attackers to cause a denial of service via a crafted RSASSA-PSS signature that lacks a mask generation function parameter.	strongswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3317
1604	CVE-2018-6412	Medium	High	In the function sbusfb_ioctl_helper() in drivers/video/fbdev/sbuslib.c in the Linux kernel through 4.15, an integer signedness error allows arbitrary information leakage for the FBIOPUTCMAP_SPARC and FBIOGETCMAP_SPARC commands.	linux	Unchanged	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3378
1605	CVE-2018-6405	Medium	Medium	In the ReadDCMImage function in coders/dcm.c in ImageMagick before 7.0.7-23, each redmap, greenmap, and bluemap variable can be overwritten by a new pointer. The previous pointer is lost, which leads to a memory leak. This allows remote attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3350
1606	CVE-2018-6392	MEDIUM	MEDIUM	The filter_slice function in libavfilter/vf_transpose.c in FFmpeg through 3.4.1 allows remote attackers to cause a denial of service (out-of-array access) via a crafted MP4 file.	ffmpeg	Unchanged	Won't Fix	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3199
1607	CVE-2018-6360	MEDIUM	HIGH	mpv through 0.28.0 allows remote attackers to execute arbitrary code via a crafted web site, because it reads HTML documents containing VIDEO elements, and accepts arbitrary URLs in a src attribute without a protocol whitelist in player/lua/ytdl_hook.lua. For example, an av://lavfi:ladspa=file= URL signifies that the product should call dlopen on a shared object file located at an arbitrary local pathname. The issue exists because the product does not consider that youtube-dl can provide a potentially unsafe URL.	mpv	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3224
1608	CVE-2018-6323	MEDIUM	HIGH	The elf_object_p function in elfcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, has an unsigned integer overflow because bfd_size_type multiplication is not used. A crafted ELF file allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.	binutils	Unchanged	8.0.0.25	9.0.0.15	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3242
1609	CVE-2018-6307	HIGH	CRITICAL	LibVNC before commit ca2a5ac02fbbadd0a21fabba779c1ea69173d10b contains heap use-after-free vulnerability in server code of file transfer extension that can result remote code execution.	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3309
1610	CVE-2018-6003	MEDIUM	HIGH	An issue was discovered in the _asn1_decode_simple_ber function in decoding.c in GNU Libtasn1 before 4.13. Unlimited recursion in the BER decoder leads to stack exhaustion and DoS.	libtasn1	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3188
1611	CVE-2018-5995	LOW	MEDIUM	The pcpu_embed_first_chunk function in mm/percpu.c in the Linux kernel through 4.14.14 allows local users to obtain sensitive address information by reading dmesg data from a pages/cpu printk call.	linux	Unchanged	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4523
1612	CVE-2018-5953	LOW	MEDIUM	The swiotlb_print_info function in lib/swiotlb.c in the Linux kernel through 4.14.14 allows local users to obtain sensitive address information by reading dmesg data from a software IO TLB printk call.	linux	Unchanged	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4548

	A	B	C	D	E	F	G	H	I	J	K	L	M
1613	CVE-2018-5873	MEDIUM	HIGH	An issue was discovered in the __ns_get_path function in fs/nsfs.c in the Linux kernel before 4.11. Due to a race condition when accessing files, a Use After Free condition can occur. This also affects all Android releases from CAF using the Linux kernel (Android for MSM, Firefox OS for MSM, QRD Android) before security patch level 2018-07-05.	linux	Unchanged	8.0.0.27	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4312
1614	CVE-2018-5848	MEDIUM	HIGH	In the function wmi_set_ie(), the length validation code does not handle unsigned integer overflow properly. As a result, a large value of the 'ie_len' argument can cause a buffer overflow in all Android releases from CAF (Android for MSM, Firefox OS for MSM, QRD Android) using the Linux Kernel.	linux	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4856
1615	CVE-2018-5814	MEDIUM	HIGH	In the Linux Kernel before version 4.16.11, 4.14.43, 4.9.102, and 4.4.133, multiple race condition errors when handling probe, disconnect, and rebind operations can be exploited to trigger a use-after-free condition or a NULL pointer dereference by sending multiple USB over IP packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4126
1616	CVE-2018-5803	MEDIUM	MEDIUM	In the Linux Kernel before version 4.15.8, 4.14.25, 4.9.87, 4.4.121, 4.1.51, and 3.2.102, an error in the _sctp_make_chunk() function (net/sctp/sm_make_chunk.c) when handling SCTP packets length can be exploited to cause a kernel crash.	linux	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4117
1617	CVE-2018-5785	MEDIUM	MEDIUM	In OpenJPEG 2.3.0, there is an integer overflow caused by an out-of-bounds left shift in the opj_j2k_setup_encoder function (openjp2/j2k.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3227
1618	CVE-2018-5784	MEDIUM	MEDIUM	In LibTIFF 4.0.9, there is an uncontrolled resource consumption in the TIFFSetDirectory function of tif_dir.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted tif file. This occurs because the declared number of directory entries is not validated against the actual number of directory entries.	libtiff	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3218
1619	CVE-2018-5766	MEDIUM	HIGH	In Libav through 12.2, there is an invalid memcpy in the av_packet_ref function of libavcodec/avpacket.c. Remote attackers could leverage this vulnerability to cause a denial of service (segmentation fault) via a crafted avi file.	libav	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3178
1620	CVE-2018-5764	MEDIUM	HIGH	The parse_arguments function in options.c in rsyncd in rsync before 3.1.3 does not prevent multiple --protect-args uses, which allows remote attackers to bypass an argument-sanitization protection mechanism.	rsync	Unchanged	8.0.0.25	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3182
1621	CVE-2018-5750	LOW	MEDIUM	The acpi_smbus_hc_add function in drivers/acpi/sbshc.c in the Linux kernel through 4.14.15 allows local users to obtain sensitive address information by reading dmesg data from an SBS HC printk call.	linux	Unchanged	8.0.0.26	9.0.0.15	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3233
1622	CVE-2018-5748	MEDIUM	HIGH	qemu/qemu_monitor.c in libvirt allows attackers to cause a denial of service (memory consumption) via a large QEMU reply.	libvirt	Unchanged	8.0.0.25	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3192
1623	CVE-2018-5745	LOW	MEDIUM	managed-keys is a feature which allows a BIND resolver to automatically maintain the keys used by trust anchors which operators configure for use in DNSSEC validation. Due to an error in the managed-keys feature it is possible for a BIND server which uses managed-keys to exit due to an assertion failure if, during key rollover, a trust anchor's keys are replaced with keys which use an unsupported algorithm. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5745.	bind	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5072
1624	CVE-2018-5744	MEDIUM	HIGH	A failure to free memory can occur when processing messages having a specific combination of EDNS options. Versions affected are: BIND 9.10.7 -> 9.10.8-P1, 9.11.3 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.10.7-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5073
1625	CVE-2018-5743	MEDIUM	HIGH	By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The number of allowed connections is a tunable parameter which, if unset, defaults to a conservative value for most servers. Unfortunately, the code which was intended to limit the number of simultaneous connections contained an error which could be exploited to grow the number of simultaneous connections beyond this limit. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.6, 9.12.0 -> 9.12.4, 9.14.0. BIND 9 Supported Preview Edition versions 9.9.3-S1 -> 9.11.5-S3, and 9.11.5-S5. Versions 9.13.0 -> 9.13.7 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5743.	bind	Unchanged	Investigate	Investigate	Investigate	10.18.44.12	10.19.45.2	10.20.3.0	LIN1018-5074
1626	CVE-2018-5741	MEDIUM	MEDIUM	ISC BIND before releases 9.11.4-P2 and 9.12.2-P2 does not properly document the behaviour of the krb5-subdomain and ms-subdomain update policies. This incorrect documentation could mislead operators into believing that policies they had configured were more restrictive than they actually were.	bind	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Vulnerable	Not vulnerable	Vulnerable	LIN10-4776
1627	CVE-2018-5740	MEDIUM	HIGH	BIND through versions 9.8.8, 9.9.13, 9.10.8, 9.11.4, 9.12.2 and 9.13.2 have a flaw in the "deny-answer-aliases" feature that can cause an INSIST assertion failure in named. A remote attacker could exploit this to cause named to crash.	bind	Unchanged	8.0.0.31	Vulnerable	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4593

	A	B	C	D	E	F	G	H	I	J	K	L	M
1628	CVE-2018-5739	Medium	HIGH	An extension to hooks capabilities which debuted in Kea 1.4.0 introduced a memory leak for operators who are using certain hooks library facilities. In order to support multiple requests simultaneously, Kea 1.4 added a callout handle store but unfortunately the initial implementation of this store does not properly free memory in every case. Hooks which make use of query4 or query6 parameters in their callouts can leak memory, resulting in the eventual exhaustion of available memory and subsequent failure of the server process. Affects Kea DHCP 1.4.0.	kea	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3530
1629	CVE-2018-5738	MEDIUM	HIGH	BIND was found to not properly handle certain configuration options, unintentionally permiting all clients to perform recursive queries. This occurs when "recursion yes;" is in effect and no match list values are provided for "allow-query-cache" or "allow-query" for the setting of "allow-recursion" to inherit a setting of all hosts from the "allow-query" setting default.	bind	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4273
1630	CVE-2018-5737	MEDIUM	HIGH	BIND versions 9.12.0 and 9.12.1 are vulnerable to problematic interaction between the serve-stale feature and NSEC aggressive negative caching can in some cases cause undesirable behavior from named, such as a recursion loop or an assertion failure resulting in termination of the named process.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4295
1631	CVE-2018-5736	LOW	MEDIUM	BIND versions 9.12.0 and 9.12.1 have an error in zone database reference counting that can lead to an assertion failure if a server attempts several transfers of a slave zone in quick succession.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4288
1632	CVE-2018-5735	MEDIUM	HIGH	It was discovered that Bind incorrectly handled DNSSEC validation. An attacker could possibly use this to cause a denial of service.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4322
1633	CVE-2018-5734	MEDIUM	HIGH	While handling a particular type of malformed packet BIND erroneously selects a SERVFAIL rcode instead of a FORMERR rcode. If the receiving view has the SERVFAIL cache feature enabled, this can trigger an assertion failure in badcache.c when the request doesn't contain all of the expected information.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4298
1634	CVE-2018-5733	MEDIUM	HIGH	A malicious client which is allowed to send very large amounts of traffic (billions of packets) to a DHCP server can eventually overflow a 32-bit reference counter, potentially causing dhcpd to crash.	dhcp	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4315
1635	CVE-2018-5732	MEDIUM	HIGH	Failure to properly bounds check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section.	dhcp	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4285
1636	CVE-2018-5730	MEDIUM	LOW	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to circumvent a DN containership check by supplying both a linkdn and containerdn database argument, or by supplying a DN string which is a left extension of a container DN string but is not hierarchically within the container DN.	krb5	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3562
1637	CVE-2018-5729	MEDIUM	MEDIUM	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to cause a denial of service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal to the database module.	krb5	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3526
1638	CVE-2018-5727	MEDIUM	MEDIUM	In OpenJPEG 2.3.0, there is an integer overflow vulnerability in the opj_t1_encode_cblks function (openjp2/t1.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.	openjpeg	Unchanged	Won't Fix	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3235
1639	CVE-2018-5712	MEDIUM	MEDIUM	An issue was discovered in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1. There is Reflected XSS on the PHAR 404 error page via the URI of a request for a .phar file.	php	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3187
1640	CVE-2018-5711	MEDIUM	MEDIUM	gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1, has an integer signedness error that leads to an infinite loop via a crafted GIF file, as demonstrated by a call to the imagecreatefromgif or imagecreatefromstring PHP function. This is related to GetCode_ and gdImageCreateFromGifCtx.	libgd&php	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3204
1641	CVE-2018-5710	MEDIUM	MEDIUM	An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. The pre-defined function strlen is getting a NULL string as a parameter value in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the Key Distribution Center (KDC), which allows remote authenticated users to cause a denial of service (NULL pointer dereference) via a modified kadmin client.	krb5	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3226
1642	CVE-2018-5709	MEDIUM	HIGH	An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable dbentry->n_key_data in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a u4 variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	krb5	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Vulnerable	LIN10-3239
1643	CVE-2018-5704	HIGH	CRITICAL	Open On-Chip Debugger (OpenOCD) 0.10.0 does not block attempts to use HTTP POST for sending data to 127.0.0.1 port 4444, which allows remote attackers to conduct cross-protocol scripting attacks, and consequently execute arbitrary commands, via a crafted web site.	openocd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3195
1644	CVE-2018-5703	HIGH	CRITICAL	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.14.11 allows attackers to cause a denial of service (slab out-of-bounds write) or possibly have unspecified other impact via vectors involving TLS.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3244

	A	B	C	D	E	F	G	H	I	J	K	L	M
1645	CVE-2018-5684	MEDIUM	HIGH	In Libav 12.1, there is an invalid memcpy call in the ff_mov_read_stsd_entries function of libavformat/mov.c. Remote attackers could leverage this vulnerability to cause a denial of service (segmentation fault) and program failure with a crafted avi file.	libav	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3098
1646	CVE-2018-5683	LOW	MEDIUM	The vga_draw_text function in Qemu allows local OS guest privileged users to cause a denial of service (out-of-bounds read and QEMU process crash) by leveraging improper memory address validation.	qemu	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3181
1647	CVE-2018-5407	LOW	MEDIUM	A flaw was found in the Intel processor execution engine sharing on SMT (e.g. Hyper-Threading) architectures. An attacker running a malicious process on the same core of the processor as the victim process, can extract certain secret information. The reporter is able to steal an OpenSSL (<= 1.1.0h) P-384 private key from a TLS server using this new side-channel vector. It is a local attack in the sense that the malicious process must be running on the same physical core as the victim (an openSSL-powered TLS server in this case). But in general any application which branches on a secret value may be affected.	openssl	Unchanged	8.0.0.29	9.0.0.20	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4951
1648	CVE-2018-5391	HIGH	HIGH	A flaw named FragmentSmack was found in the way the Linux kernel handled reassembly of fragmented IPv4 and IPv6 packets. A remote attacker could use this flaw to trigger time and calculation expensive fragment reassembly algorithms by sending specially crafted packets which could lead to a CPU saturation and hence a denial of service on the system.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4365
1649	CVE-2018-5390	HIGH	HIGH	Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4366
1650	CVE-2018-5388	MEDIUM	MEDIUM	In stroke_socket.c in strongSwan before 5.6.3, a missing packet length check could allow a buffer underflow, which may lead to resource exhaustion and denial of service while reading from the socket.	strongswan	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4103
1651	CVE-2018-5381	MEDIUM	HIGH	The Quagga BGP daemon (bgpd) prior to version 1.2.3 has a bug in its parsing of Capabilities in BGP OPEN messages, in the bgp_packet.c:bgp_capability_msg_parse function. The parser can enter an infinite loop on invalid capabilities if a Multi-Protocol capability does not have a recognized AFI/SAFI, causing a denial of service.	quagga	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3384
1652	CVE-2018-5380	MEDIUM	MEDIUM	The Quagga BGP daemon (bgpd) prior to version 1.2.3 can overrun internal BGP code-to-string conversion tables used for debug by 1 pointer value, based on input.	quagga	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3424
1653	CVE-2018-5379	HIGH	CRITICAL	The Quagga BGP daemon (bgpd) prior to version 1.2.3 can double-free memory when processing certain forms of UPDATE message, containing cluster-list and/or unknown attributes. A successful attack could cause a denial of service or potentially allow an attacker to execute arbitrary code.	quagga	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3383
1654	CVE-2018-5378	MEDIUM	MEDIUM	The Quagga BGP daemon (bgpd) prior to version 1.2.3 does not properly bounds check the data sent with a NOTIFY to a peer, if an attribute length is invalid. Arbitrary data from the bgpd process may be sent over the network to a peer and/or bgpd may crash.	quagga	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3334
1655	CVE-2018-5360	MEDIUM	HIGH	LibTIFF 4.0.9 mishandles the reading of TIFF files, as demonstrated by a heap-based buffer over-read in the ReadTIFFImage function in coders/tiff.c in GraphicsMagick 1.3.27.	libtiff	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3072
1656	CVE-2018-5358	MEDIUM	MEDIUM	ImageMagick 7.0.7-22 Q16 has memory leaks in the EncodeImageAttributes function in coders/json.c, as demonstrated by the ReadPSDLayersInternal function in coders/psd.c.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3052
1657	CVE-2018-5357	MEDIUM	MEDIUM	ImageMagick 7.0.7-22 Q16 has memory leaks in the ReadDCMImage function in coders/dcm.c.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3082
1658	CVE-2018-5344	MEDIUM	HIGH	In the Linux kernel through 4.14.13, drivers/block/loop.c mishandles lo_release serialization, which allows attackers to cause a denial of service (__lock_acquire use-after-free) or possibly have unspecified other impact.	linux	Unchanged	8.0.0.26	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3101
1659	CVE-2018-5336	MEDIUM	MEDIUM	In Wireshark 2.4.0 to 2.4.3 and 2.2.0 to 2.2.11, the JSON, XML, NTP, XMPP, and GDB dissectors could crash. This was addressed in epan/tvbparse.c by limiting the recursion depth.	wireshark	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3090
1660	CVE-2018-5335	MEDIUM	MEDIUM	In Wireshark 2.4.0 to 2.4.3 and 2.2.0 to 2.2.11, the WCP dissector could crash. This was addressed in epan/dissectors/packet-wcp.c by validating the available buffer length.	wireshark	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3083
1661	CVE-2018-5334	MEDIUM	MEDIUM	In Wireshark 2.4.0 to 2.4.3 and 2.2.0 to 2.2.11, the IxVeriWave file parser could crash. This was addressed in wiretap/vwr.c by correcting the signature timestamp bounds checks.	wireshark	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3093
1662	CVE-2018-5333	MEDIUM	MEDIUM	In the Linux kernel through 4.14.13, the rds_cmsg_atomic function in net/rds/rdma.c mishandles cases where page pinning fails or an invalid address is supplied, leading to an rds_atomic_free_op NULL pointer dereference.	linux	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3066
1663	CVE-2018-5332	HIGH	HIGH	In the Linux kernel through 4.14.13, the rds_message_alloc_sgs() function does not validate a value that is used during DMA page allocation, leading to a heap-based out-of-bounds write (related to the rds_rdma_extra_size function in net/rds/rdma.c).	linux	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3097
1664	CVE-2018-5269	MEDIUM	MEDIUM	In OpenCV 3.3.1, an assertion failure happens in cv::RBaseStream::setPos in modules/imgcodecs/src/bitstrm.cpp because of an incorrect integer cast.	opencv	Unchanged	Won't Fix	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3094
1665	CVE-2018-5268	MEDIUM	MEDIUM	In OpenCV 3.3.1, a heap-based buffer overflow happens in cv::Jpeg2KDecoder::readComponent8u in modules/imgcodecs/src/grfmt_jpeg2000.cpp when parsing a crafted image file.	opencv	Unchanged	Won't Fix	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3074

	A	B	C	D	E	F	G	H	I	J	K	L	M
1666	CVE-2018-5248	MEDIUM	HIGH	In ImageMagick 7.0.7-17 Q16, there is a heap-based buffer over-read in coders/sixel.c in the ReadSIXELImage function, related to the sixel_decode function.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3073
1667	CVE-2018-5247	MEDIUM	MEDIUM	In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadRLAImage in coders/rla.c.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3091
1668	CVE-2018-5246	MEDIUM	MEDIUM	In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadPATTERNImage in coders/pattern.c.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3095
1669	CVE-2018-5208	HIGH	CRITICAL	In Irssi before 1.0.6, a calculation error in the completion code could cause a heap buffer overflow when completing certain strings.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3078
1670	CVE-2018-5207	MEDIUM	HIGH	When using an incomplete variable argument, Irssi before 1.0.6 may access data beyond the end of the string.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3109
1671	CVE-2018-5206	HIGH	CRITICAL	When the channel topic is set without specifying a sender, Irssi before 1.0.6 may dereference a NULL pointer.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3102
1672	CVE-2018-5205	MEDIUM	HIGH	When using incomplete escape codes, Irssi before 1.0.6 may access data beyond the end of the string.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3088
1673	CVE-2018-5146	MEDIUM	HIGH	Codebooks that are not an exact divisor of the partition size are now truncated to fit within the partition.	libvorbis	Unchanged	8.0.0.27	9.0.0.17	Investigate	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4039
1674	CVE-2018-4700			A flaw was found in the CUPS printing server. Insufficient randomness makes session cookies predictable, breaking CSRF protection.	cups	Updated	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3303
1675	CVE-2018-4300	Medium	MEDIUM	The session cookie generated by the CUPS web interface was easy to guess on Linux, allowing unauthorized scripted access to the web interface when the web interface is enabled. This issue affected versions prior to v2.2.10.	cups	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3880
1676	CVE-2018-4183	HIGH	HIGH	The sandbox profile dynamically generated by cupsdCreateProfile() unintentionally allows write access to /etc/cups. This can be used by an attacker that has obtained sandboxed root access to alter /etc/cups/cups-files.conf, leading to unsandboxed root code execution.	cups	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4551
1677	CVE-2018-4182	HIGH	HIGH	It is possible to cause cups-exec to execute backends without a sandbox profile by causing cupsdCreateProfile() to fail. An attacker that has obtained sandboxed root access can accomplish this by setting the CUPS temporary directory to immutable using chflags, which will prevent the profile from being written to disk.	cups	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4524
1678	CVE-2018-4181	MEDIUM	MEDIUM	It was found that a local attacker can perform limited reads of arbitrary files as root by manipulating cupsd.conf.	cups	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4530
1679	CVE-2018-4180	MEDIUM	HIGH	Affected versions of CUPS allow for the SetEnv and PassEnv directives to be specified in the cupsd.conf file, which is editable by non-root users using the cupsctl binary. This allows attacker-controlled environment variables to be passed to CUPS backends, some of which are run as root. By passing malicious values in environment variables to affected backends, it is possible to execute an attacker-supplied binary as root, subject to sandbox restrictions.	cups	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4544
1680	CVE-2018-4022	MEDIUM	HIGH	A use-after-free vulnerability exists in the way MKVToolNix MKVINFO v25.0.0 handles the MKV (matroska) file format. A specially crafted MKV file can cause arbitrary code execution in the context of the current user.	mkvtoolnix	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-7655
1681	CVE-2018-3968	MEDIUM	HIGH	An exploitable vulnerability exists in the verified boot protection of the Das U-Boot from version 2013.07-rc1 to 2014.07-rc2. The affected versions lack proper FIT signature enforcement, which allows an attacker to bypass U-Boot's verified boot and execute an unsigned kernel, embedded in a legacy image format. To trigger this vulnerability, a local attacker needs to be able to supply the image to boot.	u-boot	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3801
1682	CVE-2018-3693	MEDIUM	MEDIUM	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a speculative buffer overflow and side-channel analysis.	linux	Unchanged	8.0.0.30	9.0.0.19	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4340
1683	CVE-2018-3665	MEDIUM	MEDIUM	System software utilizing Lazy FP state restore technique on systems using Intel Core-based microprocessors may potentially allow a local process to infer data from another process through a speculative execution side channel.	linux	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4235
1684	CVE-2018-3646	MEDIUM	MEDIUM	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.	linux	Unchanged	8.0.0.30	9.0.0.18	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4573
1685	CVE-2018-3640	MEDIUM	MEDIUM	Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis, aka Rogue System Register Read (RSRE), Variant 3a.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3958
1686	CVE-2018-3639	MEDIUM	MEDIUM	Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.	linux	Unchanged	8.0.0.29	9.0.0.18	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-3957
1687	CVE-2018-3620	MEDIUM	MEDIUM	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis.	linux	Unchanged	8.0.0.30	9.0.0.18	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4572
1688	CVE-2018-3615	MEDIUM	MEDIUM	Systems with microprocessors utilizing speculative execution and Intel software guard extensions (Intel SGX) may allow unauthorized disclosure of information residing in the L1 data cache from an enclave to an attacker with local user access via a side-channel analysis.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4571

	A	B	C	D	E	F	G	H	I	J	K	L	M
1689	CVE-2018-3286	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4869
1690	CVE-2018-3285	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Windows). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4880
1691	CVE-2018-3284	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4936
1692	CVE-2018-3283	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Logging). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4921
1693	CVE-2018-3282	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4865
1694	CVE-2018-3280	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: JSON). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4905
1695	CVE-2018-3279	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4877
1696	CVE-2018-3278	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: RBR). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4911

	A	B	C	D	E	F	G	H	I	J	K	L	M
1697	CVE-2018-3277	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4878
1698	CVE-2018-3276	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4940
1699	CVE-2018-3258	MEDIUM	HIGH	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4884
1700	CVE-2018-3251	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4866
1701	CVE-2018-3247	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Merge). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4935
1702	CVE-2018-3214	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Sound). Supported versions that are affected are Java SE: 6u201, 7u191 and 8u182; Java SE Embedded: 8u181; JRockit: R28.3.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10008
1703	CVE-2018-3212	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Information Schema). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4870

	A	B	C	D	E	F	G	H	I	J	K	L	M
1704	CVE-2018-3211	LOW	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Serviceability). Supported versions that are affected are Java SE: 8u182 and 11; Java SE Embedded: 8u181. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Java SE, Java SE Embedded executes to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data as well as unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). This vulnerability can only be exploited when Java Usage Tracker functionality is being used. CVSS 3.0 Base Score 6.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9969
1705	CVE-2018-3209	MEDIUM	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). The supported version that is affected is Java SE: 8u182. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10013
1706	CVE-2018-3203	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4889
1707	CVE-2018-3200	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4932
1708	CVE-2018-3195	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4868
1709	CVE-2018-3187	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4939

	A	B	C	D	E	F	G	H	I	J	K	L	M
1710	CVE-2018-3186	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4923
1711	CVE-2018-3185	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4902
1712	CVE-2018-3183	MEDIUM	CRITICAL	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Scripting). Supported versions that are affected are Java SE: 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10023
1713	CVE-2018-3182	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4897
1714	CVE-2018-3180	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SSL/TLS to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9955
1715	CVE-2018-3174	LOW	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4914

	A	B	C	D	E	F	G	H	I	J	K	L	M
1716	CVE-2018-3173	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4908
1717	CVE-2018-3171	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4883
1718	CVE-2018-3170	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4899
1719	CVE-2018-3169	MEDIUM	HIGH	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9937
1720	CVE-2018-3162	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4917
1721	CVE-2018-3161	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4903
1722	CVE-2018-3157	MEDIUM	LOW	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Sound). The supported version that is affected is Java SE: 11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9959

	A	B	C	D	E	F	G	H	I	J	K	L	M
1723	CVE-2018-3156	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4900
1724	CVE-2018-3155	MEDIUM	HIGH	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4924
1725	CVE-2018-3150	MEDIUM	LOW	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Utility). The supported version that is affected is Java SE: 11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10015
1726	CVE-2018-3149	MEDIUM	HIGH	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9982
1727	CVE-2018-3145	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4898
1728	CVE-2018-3144	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4885

	A	B	C	D	E	F	G	H	I	J	K	L	M
1729	CVE-2018-3143	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4934
1730	CVE-2018-3139	LOW	LOW	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10017
1731	CVE-2018-3137	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4876
1732	CVE-2018-3136	LOW	LOW	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.4 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9979
1733	CVE-2018-3133	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4926
1734	CVE-2018-3123	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: libmysqld). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3963

	A	B	C	D	E	F	G	H	I	J	K	L	M
1735	CVE-2018-3084	Low	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell: Core / Client). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 2.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4415
1736	CVE-2018-3082	Medium	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4463
1737	CVE-2018-3081	Medium	MEDIUM	Vulnerability in the MySQL Client component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4402
1738	CVE-2018-3080	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4470
1739	CVE-2018-3079	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: innoDB). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4469
1740	CVE-2018-3078	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4474
1741	CVE-2018-3077	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4476
1742	CVE-2018-3075	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4454

	A	B	C	D	E	F	G	H	I	J	K	L	M
1743	CVE-2018-3074	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4472
1744	CVE-2018-3073	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4406
1745	CVE-2018-3071	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Audit Log). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4452
1746	CVE-2018-3070	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4399
1747	CVE-2018-3067	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4426
1748	CVE-2018-3066	Medium	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N).	mysql	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4411
1749	CVE-2018-3065	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4471
1750	CVE-2018-3064	Medium	HIGH	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4475

	A	B	C	D	E	F	G	H	I	J	K	L	M
1751	CVE-2018-3063	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.60 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4468
1752	CVE-2018-3062	Low	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via memcached to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4427
1753	CVE-2018-3061	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4416
1754	CVE-2018-3060	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4403
1755	CVE-2018-3058	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: MyISAM). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4460
1756	CVE-2018-3056	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4455
1757	CVE-2018-3054	Medium	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4451

	A	B	C	D	E	F	G	H	I	J	K	L	M
1758	CVE-2018-2973	Medium	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SSL/TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).	jdk&jre		Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9590
1759	CVE-2018-2972	Medium	MEDIUM	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). The supported version that is affected is Java SE: 10.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	jdk&jre		Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9594
1760	CVE-2018-2964	Medium	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u172 and 10.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre		Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9598
1761	CVE-2018-2952	Medium	LOW	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171; JRockit: R28.3.18. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre		Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9507
1762	CVE-2018-2942	Medium	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Windows DLL). Supported versions that are affected are Java SE: 7u181 and 8u172. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre		Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9530

	A	B	C	D	E	F	G	H	I	J	K	L	M
1763	CVE-2018-2941	Medium	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). Supported versions that are affected are Java SE: 7u181, 8u172 and 10.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9511
1764	CVE-2018-2940	Medium	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9563
1765	CVE-2018-2938	Medium	CRITICAL	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Java DB). Supported versions that are affected are Java SE: 6u191, 7u181 and 8u172. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. While the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVE-2018-2938 addresses CVE-2018-1313. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9548
1766	CVE-2018-2846	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3838
1767	CVE-2018-2826	MEDIUM	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). The supported version that is affected is Java SE: 10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9114

	A	B	C	D	E	F	G	H	I	J	K	L	M
1768	CVE-2018-2825	MEDIUM	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). The supported version that is affected is Java SE: 10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9119
1769	CVE-2018-2819	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3811
1770	CVE-2018-2818	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3847
1771	CVE-2018-2817	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3804
1772	CVE-2018-2816	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3817
1773	CVE-2018-2815	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9104

	A	B	C	D	E	F	G	H	I	J	K	L	M
1774	CVE-2018-2814	MEDIUM	HIGH	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9112
1775	CVE-2018-2813	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3797
1776	CVE-2018-2812	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3796
1777	CVE-2018-2811	LOW	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Install). Supported versions that are affected are Java SE: 8u162 and 10. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: Applies to installation process on client deployment of Java. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9095
1778	CVE-2018-2810	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3872
1779	CVE-2018-2805	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: GIS Extension). Supported versions that are affected are 5.6.39 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3830

	A	B	C	D	E	F	G	H	I	J	K	L	M
1780	CVE-2018-2800	MEDIUM	MEDIUM	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u181, 7u171 and 8u162; JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, JRockit accessible data as well as unauthorized read access to a subset of Java SE, JRockit accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9111
1781	CVE-2018-2799	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9117
1782	CVE-2018-2798	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9154
1783	CVE-2018-2797	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JMX). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9141
1784	CVE-2018-2796	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9139

	A	B	C	D	E	F	G	H	I	J	K	L	M
1785	CVE-2018-2795	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9143
1786	CVE-2018-2794	LOW	HIGH	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162, 10 and JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, JRockit executes to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9105
1787	CVE-2018-2790	LOW	LOW	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9159
1788	CVE-2018-2787	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3814
1789	CVE-2018-2786	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3851

	A	B	C	D	E	F	G	H	I	J	K	L	M
1790	CVE-2018-2784	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3815
1791	CVE-2018-2783	MEDIUM	HIGH	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u161 and 8u152; Java SE Embedded: 8u152; JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9100
1792	CVE-2018-2782	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3854
1793	CVE-2018-2781	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3795
1794	CVE-2018-2780	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3798
1795	CVE-2018-2779	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3818
1796	CVE-2018-2778	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3865

	A	B	C	D	E	F	G	H	I	J	K	L	M
1797	CVE-2018-2777	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3870
1798	CVE-2018-2776	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Group Replication GCS). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via XCom to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3849
1799	CVE-2018-2775	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3820
1800	CVE-2018-2773	LOW	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3828
1801	CVE-2018-2771	LOW	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Locking). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3831
1802	CVE-2018-2769	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3864
1803	CVE-2018-2767	Low	LOW	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4459
1804	CVE-2018-2766	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3866

	A	B	C	D	E	F	G	H	I	J	K	L	M
1805	CVE-2018-2762	LOW	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3848
1806	CVE-2018-2761	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3816
1807	CVE-2018-2759	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3852
1808	CVE-2018-2758	MEDIUM	MEDIUM	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3825
1809	CVE-2018-2755	LOW	HIGH	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	mysql	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3845
1810	CVE-2018-2703	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3208
1811	CVE-2018-2696	High	High	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3217

	A	B	C	D	E	F	G	H	I	J	K	L	M
1812	CVE-2018-2678	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8687
1813	CVE-2018-2677	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8622
1814	CVE-2018-2668	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.25	9.0.0.15	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3202
1815	CVE-2018-2667	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3243
1816	CVE-2018-2665	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.25	9.0.0.15	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3183

	A	B	C	D	E	F	G	H	I	J	K	L	M
1817	CVE-2018-2663	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8629
1818	CVE-2018-2657	MEDIUM	MEDIUM	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u171 and 7u161; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, JRockit. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8654
1819	CVE-2018-2647	High	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3175
1820	CVE-2018-2646	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3177
1821	CVE-2018-2645	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3203
1822	CVE-2018-2641	LOW	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 6.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:N).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8667

	A	B	C	D	E	F	G	H	I	J	K	L	M
1823	CVE-2018-2640	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.25	9.0.0.15	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3197
1824	CVE-2018-2639	MEDIUM	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u152 and 9.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8665
1825	CVE-2018-2638	MEDIUM	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 8u152 and 9.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8624
1826	CVE-2018-2637	MEDIUM	HIGH	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JMX). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8603
1827	CVE-2018-2634	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JGSS). Supported versions that are affected are Java SE: 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8662

	A	B	C	D	E	F	G	H	I	J	K	L	M
1828	CVE-2018-2633	MEDIUM	HIGH	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8617
1829	CVE-2018-2629	LOW	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JGSS). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8644
1830	CVE-2018-2627	LOW	HIGH	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Installer). Supported versions that are affected are Java SE: 8u152 and 9.0.1. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to the Windows installer only. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8650
1831	CVE-2018-2622	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.25	9.0.0.15	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3209
1832	CVE-2018-2618	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8659

	A	B	C	D	E	F	G	H	I	J	K	L	M
1833	CVE-2018-2612	High	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3184
1834	CVE-2018-2603	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8646
1835	CVE-2018-2602	LOW	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: I18n). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, Java SE Embedded executes to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8684
1836	CVE-2018-2600	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3219
1837	CVE-2018-2599	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8640

	A	B	C	D	E	F	G	H	I	J	K	L	M
1838	CVE-2018-2598	Medium	LOW	Vulnerability in the MySQL Workbench component of Oracle MySQL (subcomponent: Workbench: Security: Encryption). Supported versions that are affected are 6.3.10 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Workbench. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Workbench accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4473
1839	CVE-2018-2591	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.6.38 and prior and 5.7.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3228
1840	CVE-2018-2590	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3223
1841	CVE-2018-2588	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: LDAP). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8625
1842	CVE-2018-2586	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3213
1843	CVE-2018-2585	High	High	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/Net). Supported versions that are affected are 6.9.9 and prior and 6.10.4 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3238
1844	CVE-2018-2583	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Stored Procedure). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3180

	A	B	C	D	E	F	G	H	I	J	K	L	M
1845	CVE-2018-2582	MEDIUM	MEDIUM	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 8u152 and 9.0.1; Java SE Embedded: 8u151. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8619
1846	CVE-2018-2581	MEDIUM	MEDIUM	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). Supported versions that are affected are Java SE: 7u161, 8u152 and 9.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8682
1847	CVE-2018-2579	MEDIUM	LOW	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8607
1848	CVE-2018-2576	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3210
1849	CVE-2018-2573	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3234
1850	CVE-2018-2565	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3193

	A	B	C	D	E	F	G	H	I	J	K	L	M
1851	CVE-2018-2562	High	High	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	8.0.0.25	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3179
1852	CVE-2018-21029	HIGH	CRITICAL	systemd 239 through 243 accepts any certificate signed by a trusted certificate authority for DNS over TLS. Server Name Indication (SNI) is not sent, and there is no hostname validation with the GnuTLS backend.	systemd	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Investigate	LIN1018-5177
1853	CVE-2018-21028	MEDIUM	HIGH	Boa through 0.94.14rc21 allows remote attackers to trigger a memory leak because of missing calls to the free function.	boa	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-9174
1854	CVE-2018-21027	HIGH	CRITICAL	Boa through 0.94.14rc21 allows remote attackers to trigger an out-of-memory (OOM) condition because malloc is mishandled.	boa	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-9175
1855	CVE-2018-21010	Medium	HIGH	OpenJPEG before 2.3.1 has a heap buffer overflow in color_apply_icc_profile in bin/common/color.c.	openjpeg	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	10.19.45.1	Not vulnerable	LIN1018-4858
1856	CVE-2018-21009	Medium	HIGH	Poppler before 0.76.0 has an integer overflow in Parser::makeStream in Parser.cc.	poppler	Unchanged	Won't Fix	9.0.0.24	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4857
1857	CVE-2018-21008	Medium	MEDIUM	An issue was discovered in the Linux kernel before 4.16.7. A use-after-free can be caused by the function rsi_mac80211_detach in the file drivers/net/wireless/rsi/rsi_91x_mac80211.c.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4840
1858	CVE-2018-20976	Medium	HIGH	An issue was discovered in fs/xfs/xfs_super.c in the Linux kernel before 4.18. A use after free exists, related to xfs_fs_fill_super failure.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4714
1859	CVE-2018-20969	High	HIGH	do_ed_script in pch.c in GNU patch through 2.7.6 does not block strings beginning with a ! character. NOTE: this is the same commit as for CVE-2019-13638, but the ! syntax is specific to ed, and is unrelated to a shell metacharacter.	patch	Unchanged	8.0.0.31	Investigate	10.17.41.17	10.18.44.10	10.19.45.4	10.20.3.0	LIN1018-4697
1860	CVE-2018-20961	HIGH	CRITICAL	In the Linux kernel before 4.16.4, a double free vulnerability in the f_midi_set_alt function of drivers/usb/gadget/function/f_midi.c in the f_midi driver may allow attackers to cause a denial of service or possibly have unspecified other impact.	linux	Unchanged	Not vulnerable	9.0.0.22	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4629
1861	CVE-2018-20856	MEDIUM	HIGH	An issue was discovered in the Linux kernel before 4.18.7. In block/blk-core.c, there is an __blk_drain_queue() use-after-free because a certain error case is mishandled.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4542
1862	CVE-2018-20855	LOW	MEDIUM	An issue was discovered in the Linux kernel before 4.18.7. In create_qp_common in drivers/infiniband/hw/mlx5/qp.c, mlx5_ib_create_qp_resp was never initialized, resulting in a leak of stack memory to userspace.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4543
1863	CVE-2018-20854	MEDIUM	HIGH	An issue was discovered in the Linux kernel before 4.20. drivers/phy/mscc/phy-ocelot-serdes.c has an off-by-one error with a resultant ctrl->phys out-of-bounds read.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4544
1864	CVE-2018-20852	MEDIUM	MEDIUM	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.	python	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4427
1865	CVE-2018-20847	Medium	HIGH	An improper computation of p_tx0, p_tx1, p_ty0 and p_ty1 in the function opj_get_encoding_parameters in openjp2/pi.c in OpenJPEG through 2.3.0 can lead to an integer overflow.	openjpeg	Unchanged	Won't Fix	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4359
1866	CVE-2018-20846	Medium	MEDIUM	Out-of-bounds accesses in the functions pi_next_lrcp, pi_next_rlcp, pi_next_rpcl, pi_next_pcrl, pi_next_rpcl, and pi_next_cprl in openmj2/pi.c in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).	openjpeg	Unchanged	Won't Fix	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4358
1867	CVE-2018-20845	Medium	MEDIUM	Division-by-zero vulnerabilities in the functions pi_next_pcrl, pi_next_cprl, and pi_next_rpcl in openmj2/pi.c in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).	openjpeg	Unchanged	Won't Fix	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4357
1868	CVE-2018-20843	High	HIGH	In libexpat in Expat before 2.2.7, XML input including XML names that contain a large number of colons could make the XML parser consume a high amount of RAM and CPU resources while processing (enough to be usable for denial-of-service attacks).	expat	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.9	Not vulnerable	Not vulnerable	LIN1018-4365
1869	CVE-2018-20836	High	HIGH	An issue was discovered in the Linux kernel before 4.20. There is a race condition in smp_task_timedout() and smp_task_done() in drivers/scsi/libsas/sas_expander.c, leading to a use-after-free.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4043
1870	CVE-2018-20815	High	CRITICAL	In QEMU 3.1.0, load_device_tree in device_tree.c calls the deprecated load_image function, which has a buffer overflow risk.	qemu	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4250
1871	CVE-2018-20796	Medium	HIGH	In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|(\\1\\1|t1|\\\2537)+' in grep.	glibc	Updated	None	None	None	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3784
1872	CVE-2018-20786	Medium	HIGH	libvterm through 0+bzr726, as used in Vim and other products, mishandles certain out-of-memory conditions, leading to a denial of service (application crash), related to screen.c, state.c, and vterm.c.	vim	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3802

	A	B	C	D	E	F	G	H	I	J	K	L	M
1873	CVE-2018-20784	High	CRITICAL	In the Linux kernel before 4.20.2, kernel/sched/fair.c mishandles leaf cfs_rq's, which allows attackers to cause a denial of service (infinite loop in update_blocked_averages) or possibly have unspecified other impact by inducing a high load.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3715
1874	CVE-2018-20783	Medium	HIGH	In PHP before 5.6.39, 7.x before 7.0.33, 7.1.x before 7.1.25, and 7.2.x before 7.2.13, a buffer over-read in PHAR reading functions may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse a .phar file. This is related to phar_parse_pharfile in ext/phar/phar.c.	php	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3709
1875	CVE-2018-20750	High	CRITICAL	LibVNC through 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3521
1876	CVE-2018-20749	High	CRITICAL	LibVNC before 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3572
1877	CVE-2018-20748	High	CRITICAL	LibVNC before 0.9.12 contains multiple heap out-of-bounds write vulnerabilities in libvncclient/rfbproto.c. The fix for CVE-2018-20019 was incomplete.	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3535
1878	CVE-2018-20712	MEDIUM	MEDIUM	A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	binutils	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-3407
1879	CVE-2018-20699	MEDIUM	MEDIUM	Docker Engine before 18.09 allows attackers to cause a denial of service (dockerd memory consumption) via a large integer in a --cpuset-mems or --cpuset-cpus value, related to daemon/daemon_unix.go, pkg/parsers/parsers.go, and pkg/sysinfo/sysinfo.go.	docker	Unchanged	8.0.0.30	Vulnerable	10.17.41.15	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3386
1880	CVE-2018-20685	LOW	MEDIUM	In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename.	openssh	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3412
1881	CVE-2018-20679	MEDIUM	HIGH	An issue was discovered in BusyBox before 1.30.0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and relay) allows a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to verification in udhcp_get_option() in networking/udhcp/common.c that 4-byte options are indeed 4 bytes.	busybox	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3373
1882	CVE-2018-20673	MEDIUM	MEDIUM	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for Create an array for saving the template argument values) that can trigger a heap-based buffer overflow, as demonstrated by nm.	binutils	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Vulnerable	LIN1018-3393
1883	CVE-2018-20671	Medium	MEDIUM	load_specific_debug_section in objdump.c in GNU Binutils through 2.31.1 contains an integer overflow vulnerability that can trigger a heap-based buffer overflow via a crafted section size.	binutils	Unchanged	8.0.0.30	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3402
1884	CVE-2018-20669	High	HIGH	An issue where a provided address with access_ok() is not checked was discovered in i915_gem_execbuffer2_ioctl in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the Linux kernel through 4.19.13. A local attacker can craft a malicious IOCTL function call to overwrite arbitrary kernel memory, resulting in a Denial of Service or privilege escalation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-3763
1885	CVE-2018-20662	Medium	MEDIUM	In Poppler 0.72.0, PDFDoc::setup in PDFDoc.cc allows attackers to cause a denial-of-service (application crash caused by Object.h SIGABRT, because of a wrong return value from PDFDoc::setup) by crafting a PDF file in which an xref data structure is mishandled during extractPDFSubtype processing.	poppler	Unchanged	Won't Fix	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3409
1886	CVE-2018-20657	MEDIUM	HIGH	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, has a memory leak via a crafted string, leading to a denial of service (memory consumption), as demonstrated by cxxfilt, a related issue to CVE-2018-12698.	binutils	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3414
1887	CVE-2018-20651	MEDIUM	MEDIUM	A NULL pointer dereference was discovered in elf_link_add_object_symbols in elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31.1. This occurs for a crafted ET_DYN with no program headers. A specially crafted ELF file allows remote attackers to cause a denial of service, as demonstrated by ld.	binutils	Unchanged	Not vulnerable	Not vulnerable	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3347
1888	CVE-2018-20650	MEDIUM	MEDIUM	A reachable Object::dictLookup assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to the lack of a check for the dict data type, as demonstrated by use of the FileSpec class (in FileSpec.cc) in pdfdetach.	poppler	Unchanged	Won't Fix	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3302
1889	CVE-2018-20623	MEDIUM	MEDIUM	In GNU Binutils 2.31.1, there is a use-after-free in the error function in elfcomm.c when called from the process_archive function in readelf.c via a crafted ELF file.	binutils	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-3324
1890	CVE-2018-20622	MEDIUM	MEDIUM	JasPer 2.0.14 has a memory leak in base/jas_malloc.c in libjasper.a when --output-format jp2 is used.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3311

	A	B	C	D	E	F	G	H	I	J	K	L	M
1891	CVE-2018-20584	MEDIUM	MEDIUM	JasPer 2.0.14 allows remote attackers to cause a denial of service (application hang) via an attempted conversion to the jp2 format, as demonstrated by 00 00 00 0c 6a 50 20 20 0d 0a 87 0a 00 00 00 14 66 74 79 70 6a 70 32 20 00 00 00 00 6a 70 32 20 00 00 00 2d 6a 70 32 68 00 00 00 16 69 68 64 72 00 00 00 20 00 00 00 20 00 03 07 07 00 00 00 00 00 0f 63 6f 6c 72 01 00 00 00 00 00 10 00 00 00 d8 6a 70 32 63 ff 4f ff 51 00 2f 00 00 00 08 00 20 00 00 00 20 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 20 00 00 00 00 00 00 00 00 00 03 07 01 01 07 01 01 07 01 01 ff 52 00 0c 00 00 00 01 01 00 04 04 00 01 ff 5c 00 04 40 40 ff 64 00 25 00 01 43 72 65 61 74 65 64 20 62 79 20 4f 70 65 6e 4a 50 45 47 20 76 65 72 73 69 6f 6e 20 32 2e 31 2e 30 ff 90 00 0a 00 00 00 00 60 00 01 ff 93 dc d7 00 18 80 0e 21 bf fc 2e ea b2 37 ce db f3 05 52 3f 43 2d 2b dd d7 64 e4 3d 67 ff 72 ab 35 2b f8 43 ca b3 5f ca d9 24 85 b4 59 5c 8d 25 fd 77 80 cb 78 1d 87 60 d6 f8 28 6e 8f 65 45 25 ea ff 5d bf 1a 71 13 10 a9 de e4 dd 6b 41 f7 38 dc 66 4f ff d9.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3328
1892	CVE-2018-20570	MEDIUM	MEDIUM	jp2_encode in jp2/jp2_enc.c in JasPer 2.0.14 has a heap-based buffer over-read.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3345
1893	CVE-2018-20553	MEDIUM	HIGH	Tcpreplay before 4.3.1 has a heap-based buffer over-read in get_l2len in common/get.c.	tcpreplay	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3300
1894	CVE-2018-20552	MEDIUM	HIGH	Tcpreplay before 4.3.1 has a heap-based buffer over-read in packet2tree in tree.c.	tcpreplay	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3337
1895	CVE-2018-20551	MEDIUM	MEDIUM	A reachable Object::getString assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to construction of invalid rich media annotation assets in the AnnotRichMedia class in Annot.c.	poppler	Unchanged	Won't Fix	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3335
1896	CVE-2018-20538	MEDIUM	MEDIUM	There is a use-after-free at asm/preproc.c (function pp_getline) in Netwide Assembler (NASM) 2.14rc16 that will cause a denial of service during certain finishes tests.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-3332
1897	CVE-2018-20535	MEDIUM	MEDIUM	There is a use-after-free at asm/preproc.c (function pp_getline) in Netwide Assembler (NASM) 2.14rc16 that will cause a denial of service during a line-number increment attempt.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-3344
1898	CVE-2018-20534	MEDIUM	MEDIUM	There is an illegal address access at src/pool.h (function pool_whatprovides) in libsolv.a in libsolv through 0.7.2 that will cause a denial of service.	libsolv	Unchanged	Not vulnerable	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3301
1899	CVE-2018-20533	MEDIUM	MEDIUM	There is a NULL pointer dereference at ext/testcase.c (function testcase_str2dep_complex) in libsolvext.a in libsolv through 0.7.2 that will cause a denial of service.	libsolv	Unchanged	Not vulnerable	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3325
1900	CVE-2018-20532	MEDIUM	MEDIUM	There is a NULL pointer dereference at ext/testcase.c (function testcase_read) in libsolvext.a in libsolv through 0.7.2 that will cause a denial of service.	libsolv	Unchanged	Not vulnerable	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3316
1901	CVE-2018-20511	LOW	MEDIUM	An issue was discovered in the Linux kernel before 4.18.11. The ipddp_ioctl function in drivers/net/appletalk/ipddp.c allows local users to obtain sensitive kernel address information by leveraging CAP_NET_ADMIN to read the ipddp_route dev and next fields via an SIOCFINDIPDDPRT ioctl call.	linux	Unchanged	8.0.0.29	9.0.0.20	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3292
1902	CVE-2018-20510	Low	MEDIUM	The print_binder_transaction_ilocked function in drivers/android/binder.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading *from *code *flags lines in a debugfs file.	linux	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4039
1903	CVE-2018-20509	Low	MEDIUM	The print_binder_ref_olocked function in drivers/android/binder.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading ref *desc *node lines in a debugfs file.	linux	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-4040
1904	CVE-2018-20506	Medium	HIGH	SQLite before 3.25.3, when the FTS3 extension is enabled, encounters an integer overflow (and resultant buffer overflow) for FTS3 queries in a merge operation that occurs after crafted changes to FTS3 shadow tables, allowing remote attackers to execute arbitrary code by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases). This is a different vulnerability than CVE-2018-20346.	sqlite	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3842
1905	CVE-2018-20505	Medium	HIGH	SQLite 3.25.2, when queries are run on a table with a malformed PRIMARY KEY, allows remote attackers to cause a denial of service (application crash) by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases).	sqlite	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3843
1906	CVE-2018-20483	LOW	HIGH	set_file_metadata in xattr.c in GNU Wget before 1.20.1 stores a file's origin URL in the user.xdg.origin.url metadata attribute of the extended attributes of the downloaded file, which allows local users to obtain sensitive information (e.g., credentials contained in the URL) by reading this attribute, as demonstrated by getfattr. This also applies to Referer information in the user.xdg.referrer.url metadata attribute. According to 2016-07-22 in the Wget ChangeLog, user.xdg.origin.url was partially based on the behavior of fwrite_xattr in tool_xattr.c in curl.	wget	Unchanged	Not vulnerable	Not vulnerable	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3315
1907	CVE-2018-20482	LOW	MEDIUM	GNU Tar through 1.30, when --sparse is used, mishandles file shrinkage during read access, which allows local users to cause a denial of service (infinite read loop in sparse_dump_region in sparse.c) by modifying a file that is supposed to be archived by a different user's process (e.g., a system backup running as root).	tar	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3296
1908	CVE-2018-20481	MEDIUM	MEDIUM	XRef::getEntry in XRef.cc in Poppler 0.72.0 mishandles unallocated XRef entries, which allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted PDF document, when XRefEntry::setFlag in XRef.h is called from Parser::makeStream in Parser.cc.	poppler	Unchanged	Won't Fix	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3334
1909	CVE-2018-20467	MEDIUM	MEDIUM	In coders/bmp.c in ImageMagick before 7.0.8-16, an input file can result in an infinite loop and hang, with high CPU and memory consumption. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3336

	A	B	C	D	E	F	G	H	I	J	K	L	M
1910	CVE-2018-20449	Low	MEDIUM	The hidma_chan_stats function in drivers/dma/qcom/hidma_dbg.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading callback= lines in a debugfs file.	linux	Unchanged	Not vulnerable	9.0.0.22	10.17.41.17	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3850
1911	CVE-2018-20406	MEDIUM	HIGH	Modules/_pickle.c in Python before 3.7.1 has an integer overflow via a large LONG_BINPUT value that is mishandled during a resize to twice the size attempt. This issue might cause memory exhaustion, but is only relevant if the pickle format is used for serializing tens or hundreds of gigabytes of data.	python	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3298
1912	CVE-2018-20362	Medium	MEDIUM	A NULL pointer dereference was discovered in ifilter_bank of libfaad/filtbank.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash because adding to windowed output is mishandled in the EIGHT_SHORT_SEQUENCE case.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3320
1913	CVE-2018-20361	Medium	MEDIUM	An invalid memory address dereference was discovered in the hf_assembly function of libfaad/sbr_hfadj.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3314
1914	CVE-2018-20360	Medium	MEDIUM	An invalid memory address dereference was discovered in the sbr_process_channel function of libfaad/sbr_dec.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3321
1915	CVE-2018-20359	Medium	MEDIUM	An invalid memory address dereference was discovered in the sbrDecodeSingleFramePS function of libfaad/sbr_dec.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3319
1916	CVE-2018-20358	Medium	MEDIUM	An invalid memory address dereference was discovered in the lt_prediction function of libfaad/lt_predict.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3327
1917	CVE-2018-20357	Medium	MEDIUM	A NULL pointer dereference was discovered in sbr_process_channel of libfaad/sbr_dec.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3343
1918	CVE-2018-20346	MEDIUM	HIGH	SQLite before 3.25.3, when the FTS3 extension is enabled, encounters an integer overflow (and resultant buffer overflow) for FTS3 queries that occur after crafted changes to FTS3 shadow tables, allowing remote attackers to execute arbitrary code by leveraging the ability to run arbitrary SQL statements (such as in certain WebSQL use cases), aka Magellan.	sqlite	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3299
1919	CVE-2018-20330	MEDIUM	HIGH	The tjLoadImage function in libjpeg-turbo 2.0.1 has an integer overflow with a resultant heap-based buffer overflow via a BMP image because multiplication of pitch and height is mishandled, as demonstrated by tjbench.	libjpeg-turbo	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3310
1920	CVE-2018-20217	LOW	MEDIUM	A Reachable Assertion issue was discovered in the KDC in MIT Kerberos 5 (aka krb5) before 1.17. If an attacker can obtain a krbtgt ticket using an older encryption type (single-DES, triple-DES, or RC4), the attacker can crash the KDC by making an S4U2Self request.	krb5	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3491
1921	CVE-2018-20216	MEDIUM	HIGH	QEMU can have an infinite loop in hw/rdma/vmw/pvrdma_dev_ring.c because return values are not checked (and -1 is mishandled).	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3323
1922	CVE-2018-20199	MEDIUM	MEDIUM	A NULL pointer dereference was discovered in ifilter_bank of libfaad/filtbank.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service because adding to windowed output is mishandled in the ONLY_LONG_SEQUENCE case.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3202
1923	CVE-2018-20198	MEDIUM	MEDIUM	A NULL pointer dereference was discovered in ifilter_bank of libfaad/filtbank.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service because adding to windowed output is mishandled in the LONG_START_SEQUENCE case.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3252
1924	CVE-2018-20197	MEDIUM	HIGH	There is a stack-based buffer underflow in the third instance of the calculate_gain function in libfaad/sbr_hfadj.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. A crafted input will lead to a denial of service or possibly unspecified other impact because limiting the additional noise energy level is mishandled for the G_max > G case.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3203
1925	CVE-2018-20196	MEDIUM	HIGH	There is a stack-based buffer overflow in the third instance of the calculate_gain function in libfaad/sbr_hfadj.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. A crafted input will lead to a denial of service or possibly unspecified other impact because the S_M array is mishandled.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3236
1926	CVE-2018-20195	MEDIUM	MEDIUM	A NULL pointer dereference was discovered in ic_predict of libfaad/ic_predict.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3223

	A	B	C	D	E	F	G	H	I	J	K	L	M
1927	CVE-2018-20194	MEDIUM	HIGH	There is a stack-based buffer underflow in the third instance of the calculate_gain function in libfaad/sbr_hfadj.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.8.8. A crafted input will lead to a denial of service or possibly unspecified other impact because limiting the additional noise energy level is mishandled for the G_max <= G case.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3209
1928	CVE-2018-20191	MEDIUM	HIGH	hw/rdma/vmw/pvrdma_main.c in QEMU does not implement a read operation (such as uar_read by analogy to uar_write), which allows attackers to cause a denial of service (NULL pointer dereference).	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3312
1929	CVE-2018-20169	HIGH	MEDIUM	An issue was discovered in the Linux kernel before 4.19.9. The USB subsystem mishandles size checks during the reading of an extra descriptor, related to __usb_get_extra_descriptor in drivers/usb/core/usb.c.	linux	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3227
1930	CVE-2018-20167	MEDIUM	HIGH	Terminology before 1.3.1 allows Remote Code Execution because popmedia is mishandled, as demonstrated by an unsafe cat README.md command when \e}pn is used. A popmedia control sequence can allow the malicious execution of executable file formats registered in the X desktop share MIME types (/usr/share/applications). The control sequence defers unknown file types to the handle_unknown_media() function, which executes xdg-open against the filename specified in the sequence. The use of xdg-open for all unknown file types allows executable file formats with a registered shared MIME type to be executed. An attacker can achieve remote code execution by introducing an executable file and a plain text file containing the control sequence through a fake software project (e.g., in Git or a tarball). When the control sequence is rendered (such as with cat), the executable file will be run.	terminology	Unchanged	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-7831
1931	CVE-2018-20145	MEDIUM	HIGH	Eclipse Mosquitto 1.5.x before 1.5.5 allows ACL bypass: if the option per_listener_settings was set to true, and the default listener was in use, and the default listener specified an acl_file, then the acl file was being ignored.	mosquitto	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN1018-3204
1932	CVE-2018-20126	LOW	MEDIUM	hw/rdma/vmw/pvrdma_cmd.c in QEMU allows create_cq and create_qp memory leaks because errors are mishandled.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3313
1933	CVE-2018-20125	MEDIUM	HIGH	hw/rdma/vmw/pvrdma_cmd.c in QEMU allows attackers to cause a denial of service (NULL pointer dereference or excessive memory allocation) in create_cq_ring or create_qp_rings.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3346
1934	CVE-2018-20124	LOW	MEDIUM	hw/rdma/rdma_backend.c in QEMU allows guest OS users to trigger out-of-bounds access via a PvrdmaSqWqe ring element with a large num_sge value.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	10.19.45.1	Not vulnerable	LIN1018-3291
1935	CVE-2018-20123	LOW	MEDIUM	pvrdma_realize in hw/rdma/vmw/pvrdma_main.c in QEMU has a Memory leak after an initialisation error.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3233
1936	CVE-2018-20030	High	HIGH	An error when processing the EXIF_IFD_INTEROPERABILITY and EXIF_IFD_EXIF tags within libexif version 0.6.21 can be exploited to exhaust available CPU resources.	libexif	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3789
1937	CVE-2018-20024	MEDIUM	HIGH	LibVNC before commit 4a21bbd097ef7c44bb000c3bd0907f96a10e4ce7 contains null pointer dereference in VNC client code that can result DoS.	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3338
1938	CVE-2018-20023	MEDIUM	HIGH	LibVNC before 8b06f835e259652b0ff026898014fc7297ade858 contains CWE-665: Improper Initialization vulnerability in VNC Repeater client code that allows attacker to read stack memory and can be abuse for information disclosure. Combined with another vulnerability, it can be used to leak stack memory layout and in bypassing ASLR	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3326
1939	CVE-2018-20022	MEDIUM	HIGH	LibVNC before 2f5b2ad1c6c99b1ac6482c95844a84d66bb52838 contains multiple weaknesses CWE-665: Improper Initialization vulnerability in VNC client code that allows attacker to read stack memory and can be abuse for information disclosure. Combined with another vulnerability, it can be used to leak stack memory layout and in bypassing ASLR	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3295
1940	CVE-2018-20021	HIGH	HIGH	LibVNC before commit c3115350eb8bb635d0fdb4dbbb0d0541f38ed19c contains a CWE-835: Infinite loop vulnerability in VNC client code. Vulnerability allows attacker to consume excessive amount of resources like CPU and RAM	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3317
1941	CVE-2018-20020	HIGH	CRITICAL	LibVNC before commit 7b1ef0ffc4815cab9a96c7278394152bdc89dc4d contains heap out-of-bound write vulnerability inside structure in VNC client code that can result remote code execution	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3294
1942	CVE-2018-20019	HIGH	CRITICAL	LibVNC before commit a83439b9fbe0f03c48eb94ed05729cb016f8b72f contains multiple heap out-of-bound write vulnerabilities in VNC client code that can result remote code execution	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3339
1943	CVE-2018-20002	MEDIUM	MEDIUM	The _bfd_generic_read_minisymbols function in syms.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31, has a memory leak via a crafted ELF file, leading to a denial of service (memory consumption), as demonstrated by nm.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3208
1944	CVE-2018-20001	MEDIUM	MEDIUM	In Libav 12.3, there is a floating point exception in the range_decode_culshift function (called from range_decode_bits) in libavcodec/apedec.c that will lead to remote denial of service via crafted input.	libav	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10253

	A	B	C	D	E	F	G	H	I	J	K	L	M
1945	CVE-2018-1999015	MEDIUM	MEDIUM	FFmpeg before commit 5aba5b89d0b1d73164d3b81764828bb8b20ff32a contains an out of array read vulnerability in ASF_F format demuxer that can result in heap memory reading. This attack appear to be exploitable via specially crafted ASF file that has to provided as input. This vulnerability appears to have been fixed in 5aba5b89d0b1d73164d3b81764828bb8b20ff32a and later.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4404
1946	CVE-2018-1999014	MEDIUM	MEDIUM	FFmpeg before commit bab0716c7f4793ec42e05a5aa7e80d82a0dd4e75 contains an out of array access vulnerability in MXF format demuxer that can result in DoS. This attack appear to be exploitable via specially crafted MXF file which has to be provided as input. This vulnerability appears to have been fixed in bab0716c7f4793ec42e05a5aa7e80d82a0dd4e75 and later.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4441
1947	CVE-2018-1999013	MEDIUM	MEDIUM	FFmpeg before commit a7e032a277452366771951e29fd0bf2bd5c029f0 contains a use-after-free vulnerability in the realmedia demuxer that can result in vulnerability allows attacker to read heap memory. This attack appear to be exploitable via specially crafted RM file has to be provided as input. This vulnerability appears to have been fixed in a7e032a277452366771951e29fd0bf2bd5c029f0 and later.	ffmpeg	Unchanged	Not vulnerable	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4453
1948	CVE-2018-1999012	HIGH	MEDIUM	FFmpeg before commit 9807d3976be0e92e4ece3b4b1701be894cd7c2e1 contains a CWE-835: Infinite loop vulnerability in pva format demuxer that can result in a Vulnerability that allows attackers to consume excessive amount of resources like CPU and RAM. This attack appear to be exploitable via specially crafted PVA file has to be provided as input. This vulnerability appears to have been fixed in 9807d3976be0e92e4ece3b4b1701be894cd7c2e1 and later.	ffmpeg	Unchanged	Won't Fix	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4424
1949	CVE-2018-1999011	MEDIUM	HIGH	FFmpeg before commit 2b46ebdbff1d8dec7a3d8ea280a612b91a582869 contains a Buffer Overflow vulnerability in asf_o format demuxer that can result in heap-buffer-overflow that may result in remote code execution. This attack appears to be exploitable via specially crafted ASF file that has to be provided as input to FFmpeg. This vulnerability appears to have been fixed in 2b46ebdbff1d8dec7a3d8ea280a612b91a582869 and later.	ffmpeg	Unchanged	Not vulnerable	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4382
1950	CVE-2018-1999010	HIGH	CRITICAL	FFmpeg before commit cced03dd667a5df6df8fd40d8de0bff477ee02e8 contains multiple out of array access vulnerabilities in the mms protocol that can result in attackers accessing out of bound data. This attack appear to be exploitable via network connectivity. This vulnerability appears to have been fixed in cced03dd667a5df6df8fd40d8de0bff477ee02e8 and later.	ffmpeg	Unchanged	Won't Fix	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4466
1951	CVE-2018-19985	LOW	MEDIUM	An issue was discovered in the Linux kernel. USB: hso: OOB memory access in hso_probe/hso_get_config_data	linux	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3322
1952	CVE-2018-19970	MEDIUM	MEDIUM	In phpMyAdmin before 4.8.4, an XSS vulnerability was found in the navigation tree, where an attacker can deliver a payload to a user through a crafted database/table name.	phpmyadmin	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3219
1953	CVE-2018-19969	MEDIUM	HIGH	phpMyAdmin 4.7.x and 4.8.x versions prior to 4.8.4 are affected by a series of CSRF flaws. By deceiving a user into clicking on a crafted URL, it is possible to perform harmful SQL operations such as renaming databases, creating new tables/routines, deleting designer pages, adding/deleting users, updating user passwords, killing SQL processes, etc.	phpmyadmin	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Vulnerable	LIN1018-3210
1954	CVE-2018-19968	MEDIUM	MEDIUM	An attacker can exploit phpMyAdmin before 4.8.4 to leak the contents of a local file because of an error in the transformation feature. The attacker must have access to the phpMyAdmin Configuration Storage tables, although these can easily be created in any database to which the attacker has access. An attacker must have valid credentials to log in to phpMyAdmin; this vulnerability does not allow an attacker to circumvent the login system.	phpmyadmin	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3205
1955	CVE-2018-19935	MEDIUM	HIGH	ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.	php	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3255
1956	CVE-2018-19932	MEDIUM	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.31. There is an integer overflow and infinite loop caused by the IS_CONTAINED_BY_LMA macro in elf.c.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3260
1957	CVE-2018-19931	MEDIUM	HIGH	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.31. There is a heap-based buffer overflow in bfd_elf32_swap_phdr_in in elfcode.h because the number of program headers is not restricted.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3239
1958	CVE-2018-19876	MEDIUM	MEDIUM	cairo 1.16.0, in cairo_ft_apply_variations() in cairo-ft-font.c, would free memory using a free function incompatible with WebKit's fastMalloc, leading to an application crash with a free(): invalid pointer error.	cairo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3228
1959	CVE-2018-19857	MEDIUM	CRITICAL	The CAF demuxer in modules/demux/caf.c in VideoLAN VLC media player 3.0.4 may read memory from an uninitialized pointer when processing magic cookies in CAF files, because a ReadKukiChunk() cast converts a return value to an unsigned int even if that value is negative. This could result in a denial of service and/or a potential infoleak.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3235

	A	B	C	D	E	F	G	H	I	J	K	L	M
1960	CVE-2018-19854	LOW	MEDIUM	An issue was discovered in the Linux kernel before 4.19.3. crypto_report_one() and related functions in crypto/crypto_user.c (the crypto user configuration API) do not fully initialize structures that are copied to userspace, potentially leaking sensitive memory to user programs. NOTE: this is a CVE-2013-2547 regression but with easier exploitability because the attacker does not need a capability (however, the system must have the CONFIG_CRYPTO_USER kconfig option).	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3216
1961	CVE-2018-19841	MEDIUM	MEDIUM	The function WavpackVerifySingleBlock in open_utils.c in libwavpack.a in WavPack through 5.1.0 allows attackers to cause a denial-of-service (out-of-bounds read and application crash) via a crafted WavPack Lossless Audio file, as demonstrated by wvunpack.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3221
1962	CVE-2018-19840	MEDIUM	MEDIUM	The function WavpackPackInit in pack_utils.c in libwavpack.a in WavPack through 5.1.0 allows attackers to cause a denial-of-service (resource exhaustion caused by an infinite loop) via a crafted wav audio file because WavpackSetConfiguration64 mishandles a sample rate of zero.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3217
1963	CVE-2018-19824	MEDIUM	HIGH	In the Linux kernel through 4.19.6, a local user could exploit a use-after-free in the ALSA driver by supplying a malicious USB Sound device (with zero interfaces) that is mishandled in usb_audio_probe in sound/usb/card.c.	linux	Unchanged	8.0.0.31	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3247
1964	CVE-2018-19788	HIGH	HIGH	A flaw was found in PolicyKit (aka polkit) 0.115 that allows a user with a uid greater than INT_MAX to successfully execute any systemctl command.	polkit	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN1018-3195
1965	CVE-2018-19758	MEDIUM	MEDIUM	There is a heap-based buffer over-read at wav.c in wav_write_header in libsndfile 1.0.28 that will cause a denial of service.	libsndfile1	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	10.18.44.5	10.19.45.1	Not vulnerable	LIN1018-3237
1966	CVE-2018-19755	MEDIUM	MEDIUM	There is an illegal address access at asm/preproc.c (function: is_mmacro) in Netwide Assembler (NASM) 2.14rc16 that will cause a denial of service (out-of-bounds array access) because a certain conversion can result in a negative integer.	nasm	Unchanged	8.0.0.29	Investigate	10.17.41.14	10.18.44.3	10.19.45.1	Not vulnerable	LIN1018-3212
1967	CVE-2018-19665	LOW	MEDIUM	The Bluetooth subsystem in QEMU mishandles negative values for length variables, leading to memory corruption.	qemu	Unchanged	8.0.0.29	9.0.0.20	Investigate	10.18.44.3	Investigate	Investigate	LIN1018-3196
1968	CVE-2018-19664	MEDIUM	MEDIUM	libjpeg-turbo 2.0.1 has a heap-based buffer over-read in the put_pixel_rows function in wrbmp.c, as demonstrated by djpeg.	libjpeg-turbo	Unchanged	Won't Fix	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Vulnerable	LIN1018-3224
1969	CVE-2018-19662	Medium	MEDIUM	An issue was discovered in libsndfile 1.0.28. There is a buffer over-read in the function i2alaw_array in alaw.c that will lead to a denial of service.	libsndfile1	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	10.19.45.1	Not vulnerable	LIN1018-3258
1970	CVE-2018-19661	Medium	MEDIUM	An issue was discovered in libsndfile 1.0.28. There is a buffer over-read in the function i2ulaw_array in ulaw.c that will lead to a denial of service.	libsndfile1	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	10.19.45.1	Not vulnerable	LIN1018-3215
1971	CVE-2018-19628	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.4, the ZigBee ZCL dissector could crash. This was addressed in epan/dissectors/packet-zbee-zcl-lighting.c by preventing a divide-by-zero error.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3225
1972	CVE-2018-19627	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.4 and 2.4.0 to 2.4.10, the IxVeriWave file parser could crash. This was addressed in wiretap/vwr.c by adjusting a buffer boundary.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3253
1973	CVE-2018-19626	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.4 and 2.4.0 to 2.4.10, the DCOM dissector could crash. This was addressed in epan/dissectors/packet-dcom.c by adding \0' termination.	wireshark	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3246
1974	CVE-2018-19625	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.4 and 2.4.0 to 2.4.10, the dissection engine could crash. This was addressed in epan/tvbuff_composite.c by preventing a heap-based buffer over-read.	wireshark	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3207
1975	CVE-2018-19624	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.4 and 2.4.0 to 2.4.10, the PVFS dissector could crash. This was addressed in epan/dissectors/packet-pvfs2.c by preventing a NULL pointer dereference.	wireshark	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3214
1976	CVE-2018-19623	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.4 and 2.4.0 to 2.4.10, the LBMPDM dissector could crash. In addition, a remote attacker could write arbitrary data to any memory locations before the packet-scoped memory. This was addressed in epan/dissectors/packet-lbmpdm.c by disallowing certain negative values.	wireshark	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3220
1977	CVE-2018-19622	MEDIUM	MEDIUM	In Wireshark 2.6.0 to 2.6.4 and 2.4.0 to 2.4.10, the MMSE dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-mmse.c by preventing length overflows.	wireshark	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3262
1978	CVE-2018-19608	LOW	MEDIUM	Arm Mbed TLS before 2.14.1, before 2.7.8, and before 2.1.17 allows a local unprivileged attacker to recover the plaintext of RSA decryption, which is used in RSA-without-(EC)DH(E) cipher suites.	mbedtls	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3229
1979	CVE-2018-19591	MEDIUM	HIGH	In the GNU C Library (aka glibc or libc6) through 2.28, attempting to resolve a crafted hostname via getaddrinfo() leads to the allocation of a socket descriptor that is not closed. This is related to the if_nametoindex() function.	glibc	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3250
1980	CVE-2018-19543	MEDIUM	HIGH	An issue was discovered in JasPer 2.0.14. There is a heap-based buffer over-read of size 8 in the function jp2_decode in libjasper/jp2/jp2_dec.c.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5070
1981	CVE-2018-19542	MEDIUM	MEDIUM	An issue was discovered in JasPer 2.0.14. There is a NULL pointer dereference in the function jp2_decode in libjasper/jp2/jp2_dec.c, leading to a denial of service.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5063
1982	CVE-2018-19541	MEDIUM	HIGH	An issue was discovered in JasPer 2.0.14. There is a heap-based buffer over-read of size 8 in the function jas_image_depalettize in libjasper/base/jas_image.c.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5057
1983	CVE-2018-19540	MEDIUM	HIGH	An issue was discovered in JasPer 2.0.14. There is a heap-based buffer overflow of size 1 in the function jas_icctxtdesc_input in libjasper/base/jas_icc.c.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5066
1984	CVE-2018-19539	MEDIUM	MEDIUM	An issue was discovered in JasPer 2.0.14. There is an access violation in the function jas_image_readcmpt in libjasper/base/jas_image.c, leading to a denial of service.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5065

	A	B	C	D	E	F	G	H	I	J	K	L	M
1985	CVE-2018-19519	MEDIUM	MEDIUM	In tcpdump 4.9.2, a stack-based buffer over-read exists in the print_prefix function of print-hncp.c via crafted packet data because of missing initialization.	tcpdump	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN10-5078
1986	CVE-2018-19518	HIGH	HIGH	University of Washington IMAP Toolkit 2007f on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r1.c and the tcp_aopen function in osdep/unix/tcp_unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a -oProxyCommand argument.	php	Unchanged	8.0.0.29	9.0.0.20	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-5060
1987	CVE-2018-19517	MEDIUM	MEDIUM	An issue was discovered in sysstat 12.1.1. The remap_struct function in sa_common.c has an out-of-bounds read during a memset call, as demonstrated by sadf.	sysstat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-5076
1988	CVE-2018-19492	MEDIUM	HIGH	An issue was discovered in cairo.trm in Gnuplot 5.2.5. This issue allows an attacker to conduct a buffer overflow with an arbitrary amount of data in the cairotrm_options function. This flaw is caused by a missing size check of an argument passed to the set font function. This issue occurs when the Gnuplot pngcairo terminal is used as a backend.	gnuplot	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5077
1989	CVE-2018-19491	MEDIUM	HIGH	An issue was discovered in post.trm in Gnuplot 5.2.5. This issue allows an attacker to conduct a buffer overflow with an arbitrary amount of data in the PS_options function. This flaw is caused by a missing size check of an argument passed to the set font function. This issue occurs when the Gnuplot postscript terminal is used as a backend.	gnuplot	Unchanged	8.0.0.29	9.0.0.20	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5064
1990	CVE-2018-19490	MEDIUM	HIGH	An issue was discovered in datafile.c in Gnuplot 5.2.5. This issue allows an attacker to conduct a heap-based buffer overflow with an arbitrary amount of data in df_generate_ascii_array_entry. To exploit this vulnerability, an attacker must pass an overlong string as the right bound of the range argument that is passed to the plot function.	gnuplot	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5075
1991	CVE-2018-19489	LOW	MEDIUM	A use-after-free flaw was found in the VirtFS, host directory sharing via Plan 9 File System(9pfs) support in QEMU. It could occur due to a race condition while renaming	qemu	Unchanged	8.0.0.29	9.0.0.20	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-5074
1992	CVE-2018-19486	HIGH	CRITICAL	Git before 2.19.2 on Linux and UNIX executes commands from the current working directory (as if '.' were at the end of $PATH) in certain cases involving the run_command() API and run-command.c, because there was a dangerous change from execvp to execv during 2017.	git	Unchanged	Not vulnerable	Not vulnerable	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-5068
1993	CVE-2018-19478	MEDIUM	MEDIUM	ghostscript: Attempting to open a carefully crafted PDF file results in long-running computation. Attempting to open a carefully crafted PDF results in a long-running computation. The page tree nodes are deeply nested where a child page tree node may be a descendent of multiple parents. Upstream bug:https://bugs.ghostscript.com/show_bug.cgi?id=699856 Upstream fix: http://git.ghostscript.com/?p=ghos dl.git;a=comm tdiff;h=0a7e5a1c309fa0911b89fa40996a7d55d90bace	ghostscript	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3308
1994	CVE-2018-19477	MEDIUM	HIGH	psi/zfjbig2.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because of a JBIG2Decode type confusion.	ghostscript	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-5072
1995	CVE-2018-19476	MEDIUM	HIGH	psi/zicc.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because of a setcolorspace type confusion.	ghostscript	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-5056
1996	CVE-2018-19475	MEDIUM	HIGH	psi/zdevice2.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because available stack space is not checked when the device remains the same.	ghostscript	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-5061
1997	CVE-2018-19432	MEDIUM	MEDIUM	An issue was discovered in libsndfile 1.0.28. There is a NULL pointer dereference in the function sf_write_int in sndfile.c, which will lead to a denial of service.	libsndfile1	Unchanged	Not vulnerable	9.0.0.20	10.17.41.13	10.18.44.3	10.19.45.1	Not vulnerable	LIN10-5079
1998	CVE-2018-19416	MEDIUM	HIGH	An issue was discovered in sysstat 12.1.1. The remap_struct function in sa_common.c has an out-of-bounds read during a memmove call, as demonstrated by sadf.	sysstat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-5062
1999	CVE-2018-19409	HIGH	CRITICAL	An issue was discovered in Artifex Ghostscript before 9.26. LockSafetyParams is not checked correctly if another device is used.	ghostscript	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-5073
2000	CVE-2018-19407	MEDIUM	MEDIUM	The vcpu_scan_ioapic function in arch/x86/kvm/x86.c in the Linux kernel through 4.19.2 allows local users to cause a denial of service (NULL pointer dereference and BUG) via crafted system calls that reach a situation where ioapic is uninitialized.	linux	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Vulnerable	LIN10-5054
2001	CVE-2018-19406	MEDIUM	MEDIUM	kvm_pv_send_ipi in arch/x86/kvm/lapic.c in the Linux kernel through 4.19.2 allows local users to cause a denial of service (NULL pointer dereference and BUG) via crafted system calls that reach a situation where the apic map is uninitialized.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-5052
2002	CVE-2018-19396	MEDIUM	HIGH	ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-5067
2003	CVE-2018-19395	MEDIUM	HIGH	ext/standard/var.c in PHP 5.x through 7.1.24 on Windows allows attackers to cause a denial of service (NULL pointer dereference and application crash) because com and com_safearray_proxy return NULL in com_properties_get in ext/com_dotnet/com_handlers.c, as demonstrated by a serialize call on COM(WScript.Shell).	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-5059

	A	B	C	D	E	F	G	H	I	J	K	L	M
2004	CVE-2018-19364	LOW	MEDIUM	A use-after-free flaw was found in the VirtFS, host directory sharing via Plan 9 File System(9pfs) support in QEMU. It could occur due to a race condition while accessing files on a shared host directory.	qemu	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-5036
2005	CVE-2018-19325	MEDIUM	HIGH	tcpdump 4.9.2 (and probably lower versions) is prone to a heap-based buffer over-read in the EXTRACT_32BITS function (extract.h, called from the rx_cache_find function, print-rx.c) due to improper serviceId sanitization.	tcpdump	Updated	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1019-4149
2006	CVE-2018-19295	HIGH	HIGH	Sylabs Singularity 2.4 to 2.6 allows local users to conduct Improper Input Validation attacks.	singularity	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3243
2007	CVE-2018-19217	MEDIUM	MEDIUM	In ncurses 6.1, there is a NULL pointer dereference at the function _nc_name_match that will lead to a denial of service attack.	ncurses	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN10-4992
2008	CVE-2018-19216	MEDIUM	HIGH	Netwide Assembler (NASM) before 2.13.02 has a use-after-free in detoken at asm/preproc.c.	nasm	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-5002
2009	CVE-2018-19215	MEDIUM	HIGH	Netwide Assembler (NASM) 2.14rc16 has a heap-based buffer over-read in expand_mmac_params in asm/preproc.c for the special cases of the % and $ and ! characters.	nasm	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.5	Not vulnerable	Not vulnerable	LIN10-5015
2010	CVE-2018-19214	MEDIUM	HIGH	Netwide Assembler (NASM) 2.14rc15 has a heap-based buffer over-read in expand_mmac_params in asm/preproc.c for insufficient input.	nasm	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.5	Not vulnerable	Not vulnerable	LIN10-4993
2011	CVE-2018-19213	MEDIUM	MEDIUM	Netwide Assembler (NASM) through 2.14rc16 has memory leaks that may lead to DoS, related to nasm_malloc in nasmlib/malloc.c.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	LIN10-4997
2012	CVE-2018-19211	MEDIUM	MEDIUM	In ncurses 6.1, there is a NULL pointer dereference at function _nc_parse_entry in parse_entry.c that will lead to a denial of service attack.	ncurses	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4981
2013	CVE-2018-19210	MEDIUM	MEDIUM	In LibTIFF 4.0.9, there is a NULL pointer dereference in the TIFFWriteDirectorySec function in tif_dirwrite.c that will lead to a denial of service attack, as demonstrated by tiffset.	tiff	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN10-5014
2014	CVE-2018-19209	MEDIUM	MEDIUM	Netwide Assembler (NASM) 2.14rc15 has a NULL pointer dereference in the function find_label in asm/labels.c that will lead to a DoS attack.	nasm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-5000
2015	CVE-2018-19191	Low	MEDIUM	Webmin 1.890 has XSS via /config.cgi? webmin, the /shell/index.cgi history parameter, /shell/index.cgi?stripped=1, or the /webminlog/search.cgi uall or mall parameter.	webmin	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3791
2016	CVE-2018-19149	MEDIUM	MEDIUM	Poppler before 0.70.0 has a NULL pointer dereference in _poppler_attachment_new when called from poppler_annot_file_attachment_get_attachment.	poppler	Unchanged	Won't Fix	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5009
2017	CVE-2018-19139	MEDIUM	MEDIUM	An issue has been found in JasPer 2.0.14. There is a memory leak in jas_malloc.c when called from jpc_unk_getparms in jpc_cs.c.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5017
2018	CVE-2018-19134	MEDIUM	HIGH	In Artifex Ghostscript through 9.25, the setpattern operator did not properly validate certain types. A specially crafted PostScript document could exploit this to crash Ghostscript or, possibly, execute arbitrary code in the context of the Ghostscript process. This is a type confusion issue because of failure to check whether the Implementation of a pattern dictionary was a structure type.	ghostscript	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3318
2019	CVE-2018-19132	MEDIUM	MEDIUM	Squid before 4.4, when SNMP is enabled, allows a denial of service (Memory Leak) via an SNMP packet.	squid	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4989
2020	CVE-2018-19131	MEDIUM	MEDIUM	Squid before 4.4 has XSS via a crafted X.509 certificate during HTTP(S) error page generation for certificate errors.	squid	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5021
2021	CVE-2018-19130	MEDIUM	MEDIUM	In Libav 12.3, there is an invalid memory access in vc1_decode_frame in libavcodec/vc1dec.c that allows attackers to cause a denial-of-service via a crafted aac file.	libav	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10061
2022	CVE-2018-19129	MEDIUM	MEDIUM	In Libav 12.3, a NULL pointer dereference (RIP points to zero) issue in ff_mpa_synth_filter_float in libavcodec/mpegaudiodsp_template.c can cause a segmentation fault (application crash) via a crafted mov file.	libav	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10075
2023	CVE-2018-19128	MEDIUM	MEDIUM	In Libav 12.3, there is a heap-based buffer over-read in decode_frame in libavcodec/lcldec.c that allows an attacker to cause denial-of-service via a crafted avi file.	libav	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10057
2024	CVE-2018-19115	HIGH	CRITICAL	keepalived before 2.0.7 has a heap-based buffer overflow when parsing HTTP status codes resulting in DoS or possibly unspecified other impact, because extract_status_code in lib/html.c has no validation of the status code and instead writes an unlimited amount of data to the heap.	keepalived	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5005
2025	CVE-2018-19060	MEDIUM	MEDIUM	An issue was discovered in Poppler 0.71.0. There is a NULL pointer dereference in goo/GooString.h, will lead to denial of service, as demonstrated by utils/pdfdetach.cc not validating a filename of an embedded file before constructing a save path.	poppler	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4999
2026	CVE-2018-19059	MEDIUM	MEDIUM	An issue was discovered in Poppler 0.71.0. There is a out-of-bounds read in EmbFile::save2 in FileSpec.cc, will lead to denial of service, as demonstrated by utils/pdfdetach.cc not validating embedded files before save attempts.	poppler	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4987
2027	CVE-2018-19058	MEDIUM	MEDIUM	An issue was discovered in Poppler 0.71.0. There is a reachable abort in Object.h, will lead to denial of service because EmbFile::save2 in FileSpec.cc lacks a stream check before saving an embedded file.	poppler	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5003
2028	CVE-2018-19052	MEDIUM	HIGH	An issue was discovered in mod_alias_physical_handler in mod_alias.c in lighttpd before 1.4.50. There is potential ../ path traversal of a single directory above an alias target, with a specific mod_alias configuration where the matched alias lacks a trailing '/' character, but the alias target filesystem path does have a trailing '/' character.	lighttpd	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-5011

	A	B	C	D	E	F	G	H	I	J	K	L	M
2029	CVE-2018-19046	LOW	MEDIUM	keepalived 2.0.8 didn't check for existing plain files when writing data to a temporary file upon a call to PrintData or PrintStats. If a local attacker had previously created a file with the expected name (e.g., /tmp/keepalived.data or /tmp/keepalived.stats), with read access for the attacker and write access for the keepalived process, then this potentially leaked sensitive information.	keepalived	Unchanged	Not vulnerable	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4996
2030	CVE-2018-19045	MEDIUM	HIGH	keepalived 2.0.8 used mode 0666 when creating new temporary files upon a call to PrintData or PrintStats, potentially leaking sensitive information.	keepalived	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5018
2031	CVE-2018-19044	LOW	MEDIUM	keepalived 2.0.8 didn't check for pathnames with symlinks when writing data to a temporary file upon a call to PrintData or PrintStats. This allowed local users to overwrite arbitrary files if fs.protected_symlinks is set to 0, as demonstrated by a symlink from /tmp/keepalived.data or /tmp/keepalived.stats to /etc/passwd.	keepalived	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5012
2032	CVE-2018-18956	MEDIUM	HIGH	The ProcessMimeEntity function in util-decode-mime.c in Suricata 4.x before 4.0.6 allows remote attackers to cause a denial of service (segfault and daemon crash) via crafted input to the SMTP parser, as exploited in the wild in November 2018.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4985
2033	CVE-2018-18955	MEDIUM	HIGH	userns: also map extents in the reverse map to kernel IDs	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4988
2034	CVE-2018-18954	LOW	MEDIUM	An OOB r/w buffer access issue was found in the PowerPC PowerNV LPC controller in 'pnv_lpc_do_eccb' routine. It could occur while performing a memory write operation. A guest user/process could use this flaw to crash the QEMU process resulting in DoS.	qemu	Unchanged	Not vulnerable	Not vulnerable	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4994
2035	CVE-2018-18897	MEDIUM	MEDIUM	An issue was discovered in Poppler 0.71.0. There is a memory leak in GfxColorSpace::setDisplayProfile in GfxState.cc, as demonstrated by pdftocairo.	poppler	Unchanged	Won't Fix	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4986
2036	CVE-2018-18873	MEDIUM	HIGH	An issue was discovered in JasPer 2.0.14. There is a NULL pointer dereference in the function ras_putdatastd in ras/ras_enc.c.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5006
2037	CVE-2018-18849	LOW	MEDIUM	An out of bounds memory access issue was found in the LSI53C895A SCSI Host Bus Adapter emulation while writing a message in lsi_do_msgin. It could occur during migration if the 'msg_len' field has an invalid value. A user/process could use this flaw to crash the Qemu process resulting in DoS.	qemu	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4983
2038	CVE-2018-18839	MEDIUM	MEDIUM	** DISPUTED ** An issue was discovered in Netdata 1.10.0. Full Path Disclosure (FPD) exists via api/v1/alarms. NOTE: the vendor says is intentional.	netdata	Unchanged	Not vulnerable	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-1553
2039	CVE-2018-18838	Medium	HIGH	An issue was discovered in Netdata 1.10.0. Log Injection (or Log Forgery) exists via a %0a sequence in the url parameter to api/v1/registry.	netdata	Unchanged	Not vulnerable	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4308
2040	CVE-2018-18837	Medium	MEDIUM	An issue was discovered in Netdata 1.10.0. HTTP Header Injection exists via the api/v1/data filename parameter because of web_client_api_request_v1_data in web/api/web_api_v1.c.	netdata	Unchanged	Not vulnerable	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4307
2041	CVE-2018-18836	Medium	MEDIUM	An issue was discovered in Netdata 1.10.0. JSON injection exists via the api/v1/data tqx parameter because of web_client_api_request_v1_data in web/api/web_api_v1.c.	netdata	Unchanged	Not vulnerable	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4306
2042	CVE-2018-18829	MEDIUM	MEDIUM	There exists a NULL pointer dereference in ff_vc1_parse_frame_header_adv in vc1.c in Libav 12.3, which allows attackers to cause a denial-of-service through a crafted aac file.	libav	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-10020
2043	CVE-2018-18828	MEDIUM	MEDIUM	There exists a heap-based buffer overflow in vc1_decode_i_block_adv in vc1_block.c in Libav 12.3, which allows attackers to cause a denial-of-service via a crafted aac file.	libav	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9968
2044	CVE-2018-18827	MEDIUM	MEDIUM	There exists a heap-based buffer over-read in ff_vc1_pred_dc in vc1_block.c in Libav 12.3, which allows attackers to cause a denial-of-service via a crafted aac file.	libav	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9940
2045	CVE-2018-18826	MEDIUM	MEDIUM	There exists a heap-based buffer overflow in vc1_decode_p_mb_intfi in vc1_block.c in Libav 12.3, which allows attackers to cause a denial-of-service via a crafted aac file.	libav	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9962
2046	CVE-2018-18751	HIGH	CRITICAL	An issue was discovered in GNU gettext 0.19.8. There is a double free in default_add_message in read-catalog.c, related to an invalid free in po_gram_parse in po-gram-gen.y, as demonstrated by lt-msgfmt.	gettext	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.2	Not vulnerable	Not vulnerable	LIN10-4930
2047	CVE-2018-18718	MEDIUM	HIGH	An issue was discovered in gThumb through 3.6.2. There is a double-free vulnerability in the add_themes_from_dir method in dlg-contact-sheet.c because of two successive calls of g_free, each of which frees the same buffer.	gthumb	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-7687
2048	CVE-2018-18710	LOW	MEDIUM	An issue was discovered in the Linux kernel through 4.19. An information leak in cdrom_ioctl_select_disc in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940 and CVE-2018-16658.	linux	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4941
2049	CVE-2018-18701	MEDIUM	MEDIUM	An issue was discovered in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31. There is a stack consumption vulnerability resulting from infinite recursion in the functions next_is_type_qual() and cplus_demangle_type() in cp-demangle.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via an ELF file, as demonstrated by nm.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4909
2050	CVE-2018-18700	MEDIUM	MEDIUM	An issue was discovered in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31. There is a stack consumption vulnerability resulting from infinite recursion in the functions d_name(), d_encoding(), and d_local_name() in cp-demangle.c. Remote attackers could leverage this vulnerability to cause a denial-of-service via an ELF file, as demonstrated by nm.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4912

	A	B	C	D	E	F	G	H	I	J	K	L	M
2051	CVE-2018-18690	MEDIUM	MEDIUM	In the Linux kernel before 4.17, a local attacker able to set attributes on an xfs filesystem could make this filesystem non-operational until the next mount by triggering an unchecked error condition during an xfs attribute change, because xfs_attr_shortform_addname in fs/xfs/libxfs/xfs_attr.c mishandles ATTR_REPLACE operations with conversion of an attr from short to long form.	linux	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4933
2052	CVE-2018-18661	MEDIUM	MEDIUM	An issue was discovered in LibTIFF 4.0.9. There is a NULL pointer dereference in the function LZWDecode in the file tif_lzw.c.	tiff	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4891
2053	CVE-2018-18653	HIGH	HIGH	The Linux kernel, as used in Ubuntu 18.10 and when booted with UEFI Secure Boot enabled, allows privileged local users to bypass intended Secure Boot restrictions and execute untrusted code by loading arbitrary kernel modules. This occurs because a modified kernel/module.c, in conjunction with certain configuration options, leads to mishandling of the result of signature verification.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4938
2054	CVE-2018-18607	MEDIUM	MEDIUM	An issue was discovered in elf_link_input_bfd in elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. There is a NULL pointer dereference in elf_link_input_bfd when used for finding STT_TLS symbols without any TLS section. A specially crafted ELF allows remote attackers to cause a denial of service, as demonstrated by ld.	binutils	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4904
2055	CVE-2018-18606	MEDIUM	MEDIUM	An issue was discovered in the merge_strings function in merge.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. There is a NULL pointer dereference in _bfd_add_merge_section when attempting to merge sections with large alignments. A specially crafted ELF allows remote attackers to cause a denial of service, as demonstrated by ld.	binutils	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4871
2056	CVE-2018-18605	MEDIUM	MEDIUM	A heap-based buffer over-read issue was discovered in the function sec_merge_hash_lookup in merge.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31, because _bfd_add_merge_section mishandles section merges when size is not a multiple of entsize. A specially crafted ELF allows remote attackers to cause a denial of service, as demonstrated by ld.	binutils	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4875
2057	CVE-2018-18585	MEDIUM	MEDIUM	chmd_read_headers in mspack/chmd.c in libmspack before 0.8alpha accepts a filename that has \0' as its first or second character (such as the /\0 name).	libmspack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4929
2058	CVE-2018-18584	MEDIUM	MEDIUM	In mspack/cab.h in libmspack before 0.8alpha and cabextract before 1.8, the CAB block input buffer is one byte too small for the maximal Quantum block, leading to an out-of-bounds write.	libmspack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4888
2059	CVE-2018-18559	MEDIUM	HIGH	In the Linux kernel through 4.19, a use-after-free can occur due to a race condition between fanout_add from setsockopt and bind on an AF_PACKET socket. This issue exists because of the 15fe076edea787807a7cdc168df832544b58eba6 incomplete fix for a race condition. The code mishandles a certain multithreaded case involving a packet_do_bind unregister action followed by a packet_notifier register action. Later, packet_release operates on only one of the two applicable linked lists. The attacker can achieve Program Counter control.	linux	Unchanged	8.0.0.29	9.0.0.20	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4922
2060	CVE-2018-18557	MEDIUM	HIGH	LibTIFF 4.0.9 (with JBIG enabled) decodes arbitrarily-sized JBIG into a buffer, ignoring the buffer size, which leads to a tif_jbig.c JBIGDecode out-of-bounds write.	tiff	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4918
2061	CVE-2018-18544	MEDIUM	MEDIUM	There is a memory leak in the function WriteMSLImage of coders/msl.c in ImageMagick 7.0.8-13 Q16.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4937
2062	CVE-2018-18521	MEDIUM	MEDIUM	Divide-by-zero vulnerabilities in the function arlib_add_symbols() in arlib.c in elfutils 0.174 allow remote attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by eu-ranlib, because a zero sh_entsize is mishandled.	elfutils	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4882
2063	CVE-2018-18520	MEDIUM	MEDIUM	An Invalid Memory Address Dereference exists in the function elf_end in libelf in elfutils through v0.174. Although eu-size is intended to support ar files inside ar files, handle_ar in size.c closes the outer ar file before handling all inner entries. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file.	elfutils	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4873
2064	CVE-2018-18484	MEDIUM	MEDIUM	An issue was discovered in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there is a stack consumption problem caused by recursive stack frames: cplus_demangle_type, d_bare_function_type, d_function_type.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4892
2065	CVE-2018-18483	MEDIUM	HIGH	The get_count function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31, allows remote attackers to cause a denial of service (malloc called with the result of an integer-overflowing calculation) or possibly have unspecified other impact via a crafted string, as demonstrated by c++filt.	binutils	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4896
2066	CVE-2018-18445	HIGH	HIGH	In the Linux kernel 4.14.x, 4.15.x, 4.16.x, 4.17.x, and 4.18.x before 4.18.13, faulty computation of numeric bounds in the BPF verifier permits out-of-bounds memory accesses because adjust_scalar_min_max_vals in kernel/bpf/verifier.c mishandles 32-bit right shifts.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4928
2067	CVE-2018-18440	HIGH	HIGH	DENX U-Boot through 2018.09-rc1 has a locally exploitable buffer overflow via a crafted kernel image because filesystem loading is mishandled.	u-boot	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	10.19.45.1	Not vulnerable	LIN10-5048

	A	B	C	D	E	F	G	H	I	J	K	L	M
2068	CVE-2018-18439	HIGH	CRITICAL	DENX U-Boot through 2018.09-rc1 has a remotely exploitable buffer overflow via a malicious TFTP server because TFTP traffic is mishandled. Also, local exploitation can occur via a crafted kernel image.	u-boot	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	10.19.45.1	Not vulnerable	LIN10-5049
2069	CVE-2018-18438	LOW	MEDIUM	Qemu has integer overflows because IORead Handler and its associated functions use a signed integer data type for a size value.	qemu	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Vulnerable	LIN10-4913
2070	CVE-2018-18408	HIGH	CRITICAL	A use-after-free was discovered in the tcpbridge binary of Tcpreplay 4.3.0 beta1. The issue gets triggered in the function post_args() at tcpbridge.c, causing a denial of service or possibly unspecified other impact.	tcpreplay	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4915
2071	CVE-2018-18407	MEDIUM	MEDIUM	A heap-based buffer over-read was discovered in the tcpreplay-edit binary of Tcpreplay 4.3.0 beta1, during the incremental checksum operation. The issue gets triggered in the function csum_replace4() in incremental_checksum.h, causing a denial of service.	tcpreplay	Unchanged	Not vulnerable	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4910
2072	CVE-2018-18398	LOW	MEDIUM	Xfce Thunar 1.6.15, when Xfce 4.12 is used, mishandles the IBus-Unikey input method for file searches within File Manager, leading to an out-of-bounds read and SEGV. This could potentially be exploited by an arbitrary local user who creates files in /tmp before the victim uses this input method.	thunar	Unchanged	Vulnerable	Vulnerable	Vulnerable	Investigate	Not vulnerable	Not vulnerable	LIN10-4894
2073	CVE-2018-18397	LOW	MEDIUM	The userfaultfd implementation in the Linux kernel before 4.19.7 mishandles access control for certain UFFDIO_ioctl calls, as demonstrated by allowing local users to write data into holes in a tmpfs file (if the user has read-only access to that file, and that file contains holes), related to fs/userfaultfd.c and mm/userfaultfd.c.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.14	10.18.44.3	Not vulnerable	Vulnerable	LIN1018-3240
2074	CVE-2018-18386	LOW	LOW	drivers/tty/n_tty.c in the Linux kernel before 4.14.11 allows local attackers (who are able to access pseudo terminals) to hang/block further usage of any pseudo terminal devices due to an EXTPROC versus ICANON confusion in TIOCINQ.	linux	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4859
2075	CVE-2018-18384	MEDIUM	MEDIUM	Info-ZIP UnZip 6.0 has a buffer overflow in list.c, when a ZIP archive has a crafted relationship between the compressed-size value and the uncompressed-size value, because a buffer size is 10 and is supposed to be 12.	unzip	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	10.19.45.1	Not vulnerable	LIN10-4925
2076	CVE-2018-18314	HIGH	CRITICAL	Perl before 5.26.3 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	perl	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3232
2077	CVE-2018-18313	MEDIUM	CRITICAL	Perl before 5.26.3 has a buffer over-read via a crafted regular expression that triggers disclosure of sensitive information from process memory.	perl	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3248
2078	CVE-2018-18312	HIGH	CRITICAL	Perl before 5.26.3 and 5.28.0 before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	perl	Unchanged	Not vulnerable	Not vulnerable	10.17.41.15	10.18.44.5	Not vulnerable	Vulnerable	LIN1018-3206
2079	CVE-2018-18311	HIGH	CRITICAL	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	perl	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3251
2080	CVE-2018-18310	MEDIUM	MEDIUM	An invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl in elfutils through v0.174. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by consider_notes.	elfutils	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4860
2081	CVE-2018-18309	MEDIUM	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. An invalid memory address dereference was discovered in read_reloc in reloc.c. The vulnerability causes a segmentation fault and application crash, which leads to denial of service, as demonstrated by objdump, because of missing _bfd_clear_contents bounds checking.	binutils	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4927
2082	CVE-2018-18284	HIGH	CRITICAL	Artifex Ghostscript 9.25 and earlier allows attackers to bypass a sandbox protection mechanism via vectors involving the 1Policy operator.	ghostscript	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4920
2083	CVE-2018-18281	MEDIUM	HIGH	Since Linux kernel version 3.2, the mremap() syscall performs TLB flushes after dropping pagetable locks. If a syscall such as ftruncate() removes entries from the pagetables of a task that is in the middle of mremap(), a stale TLB entry can remain for a short time that permits access to a physical page after it has been released back to the page allocator and reused. This is fixed in the following kernel versions: 4.9.135, 4.14.78, 4.18.16, 4.19.	linux	Unchanged	8.0.0.28	9.0.0.20	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4893
2084	CVE-2018-18245	LOW	MEDIUM	Nagios Core 4.4.2 has XSS via the alert summary reports of plugin results, as demonstrated by a SCRIPT element delivered by a modified check_load plugin to NRPE.	nagios-core	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	10.18.44.5	Not vulnerable	Vulnerable	LIN1018-3211
2085	CVE-2018-18227	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.3 and 2.4.0 to 2.4.9, the MS-WSP protocol dissector could crash. This was addressed in epan/dissectors/packet-mswsp.c by properly handling NULL return values.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4818
2086	CVE-2018-18226	HIGH	HIGH	In Wireshark 2.6.0 to 2.6.3, the Steam IHS Discovery dissector could consume system memory. This was addressed in epan/dissectors/packet-steam-ihs-discovery.c by changing the memory-management approach.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4819
2087	CVE-2018-18225	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.3, the CoAP dissector could crash. This was addressed in epan/dissectors/packet-coap.c by ensuring that the piv length is correctly computed.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4822
2088	CVE-2018-18088	MEDIUM	MEDIUM	OpenJPEG 2.3.0 has a NULL pointer dereference for red in the imagetopnm function of jp2/convert.c	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4781
2089	CVE-2018-18074	MEDIUM	CRITICAL	The Requests package through 2.19.1 before 2018-09-14 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.	python-requests	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4780
2090	CVE-2018-18073	MEDIUM	MEDIUM	Artifex Ghostscript allows attackers to bypass a sandbox protection mechanism by leveraging exposure of system operators in the saved execution stack in an error object.	ghostscript	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4886

	A	B	C	D	E	F	G	H	I	J	K	L	M
2091	CVE-2018-18066	MEDIUM	HIGH	snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4804
2092	CVE-2018-18065	MEDIUM	MEDIUM	_set_key in agent/helpers/table_container.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an authenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.	net-snmp	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4791
2093	CVE-2018-18064	MEDIUM	MEDIUM	cairo through 1.15.14 has an out-of-bounds stack-memory write during processing of a crafted document by WebKitGTK+ because of the interaction between cairo-rectangular-scan-converter.c (the generate and render_rows functions) and cairo-image-compositor.c (the _cairo_image_spans_and_zero function).	cairo	Unchanged	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	LIN10-4814
2094	CVE-2018-18025	MEDIUM	MEDIUM	In ImageMagick 7.0.8-13 Q16, there is a heap-based buffer over-read in the EncodeImage function of coders/pict.c, which allows attackers to cause a denial of service via a crafted SVG image file.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4798
2095	CVE-2018-18024	MEDIUM	MEDIUM	In ImageMagick 7.0.8-13 Q16, there is an infinite loop in the ReadBMPImage function of the coders/bmp.c file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4810
2096	CVE-2018-18023	MEDIUM	MEDIUM	In ImageMagick 7.0.8-13 Q16, there is a heap-based buffer over-read in the SVGStripString function of coders/svg.c, which allows attackers to cause a denial of service via a crafted SVG image file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4802
2097	CVE-2018-18021	LOW	HIGH	arch/arm64/kvm/guest.c in KVM in the Linux kernel before 4.18.12 on the arm64 platform mishandles the KVM_SET_ON_REG ioctl. This is exploitable by attackers who can create virtual machines. An attacker can arbitrarily redirect the hypervisor flow of control (with full register control). An attacker can also cause a denial of service (hypervisor panic) via an illegal exception return. This occurs because of insufficient restrictions on userspace access to the core register file, and because PSTATE.M validation does not prevent unintended execution modes.	linux	Unchanged	8.0.0.29	9.0.0.20	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4796
2098	CVE-2018-18016	MEDIUM	MEDIUM	ImageMagick 7.0.7-28 has a memory leak vulnerability in WritePCXImage in coders/pcx.c.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4809
2099	CVE-2018-17985	MEDIUM	MEDIUM	An issue was discovered in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31. There is a stack consumption problem caused by the cplus_demangle_type function making recursive calls to itself in certain scenarios involving many 'P' characters.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4808
2100	CVE-2018-17983	MEDIUM	CRITICAL	cext/manifest.c in Mercurial before 4.7.2 has an out-of-bounds read during parsing of a malformed manifest entry.	mercurial	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4813
2101	CVE-2018-17977	MEDIUM	MEDIUM	The Linux kernel 4.14.67 mishandles certain interaction among XFRM Netlink messages, IPPROTO_AH packets, and IPPROTO_IP packets, which allows local users to cause a denial of service (memory consumption and system hang) by leveraging root access to execute crafted applications, as demonstrated on CentOS 7.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Investigate	Not vulnerable	Not vulnerable	LIN10-4795
2102	CVE-2018-17974	MEDIUM	MEDIUM	An issue was discovered in Tcpreplay 4.3.0 beta1. A heap-based buffer over-read was triggered in the function dlt_en10mb_encode() of the file plugins/dlt_en10mb/en10mb.c, due to inappropriate values in the function memmove(). The length (pktlen + ctx -> l2len) can be larger than source value (packet + ctx->l2len) because the function fails to ensure the length of a packet is valid. This leads to Denial of Service.	tcpreplay	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4805
2103	CVE-2018-17972	MEDIUM	MEDIUM	An issue was discovered in the proc_pid_stack function in fs/proc/base.c in the Linux kernel through 4.18.11. It does not ensure that only root may inspect the kernel stack of an arbitrary task, allowing a local attacker to exploit racy stack unwinding and leak kernel task stack contents.	linux	Unchanged	8.0.0.30	9.0.0.20	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4807
2104	CVE-2018-17967	MEDIUM	MEDIUM	ImageMagick 7.0.7-28 has a memory leak vulnerability in ReadBGRImage in coders/bgr.c.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4787
2105	CVE-2018-17966	MEDIUM	MEDIUM	ImageMagick 7.0.7-28 has a memory leak vulnerability in WritePDBImage in coders/pdb.c.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4797
2106	CVE-2018-17965	MEDIUM	MEDIUM	ImageMagick 7.0.7-28 has a memory leak vulnerability in WriteSGIImage in coders/sgi.c.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4815
2107	CVE-2018-17963	HIGH	CRITICAL	qemu_deliver_packet_iov in net/net.c in Qemu accepts packet sizes greater than INT_MAX, which allows attackers to cause a denial of service or possibly have unspecified other impact.	qemu	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4820
2108	CVE-2018-17962	MEDIUM	HIGH	Qemu has a Buffer Overflow in pcnet_receive in hw/net/pcnet.c because an incorrect integer data type is used.	qemu	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4817
2109	CVE-2018-17961	MEDIUM	HIGH	Artifex Ghostscript 9.25 and earlier allows attackers to bypass a sandbox protection mechanism via vectors involving errorhandler setup. NOTE: this issue exists because of an incomplete fix for CVE-2018-17183.	ghostscript	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4864
2110	CVE-2018-17958	MEDIUM	HIGH	Qemu has a Buffer Overflow in rtl8139_do_receive in hw/net/rtl8139.c because an incorrect integer data type is used.	qemu	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4783
2111	CVE-2018-17953	HIGH	HIGH	A incorrect variable in a SUSE specific patch for pam_access rule matching in PAM 1.3.0 in openSUSE Leap 15.0 and SUSE Linux Enterprise 15 could lead to pam_access rules not being applied (fail open).	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3263
2112	CVE-2018-17942	MEDIUM	HIGH	The convert_to_decimal function in vasnprintf.c in Gnulib before 2018-09-23 has a heap-based buffer overflow because memory is not allocated for a trailing '\0' character during %f processing.	gnulib	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4788

	A	B	C	D	E	F	G	H	I	J	K	L	M
2113	CVE-2018-17937	Medium	HIGH	gpsd versions 2.90 to 3.17 and microjson versions 1.0 to 1.3, an open source project, allow a stack-based buffer overflow, which may allow remote attackers to execute arbitrary code on embedded platforms via traffic on Port 2947/TCP or crafted JSON inputs.	gpsd	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3798
2114	CVE-2018-17795	MEDIUM	HIGH	The function t2p_write_pdf in tiff2pdf.c in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted TIFF file, a similar issue to CVE-2017-9935.	tiff	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.2	Not vulnerable	Not vulnerable	LIN10-4816
2115	CVE-2018-17794	MEDIUM	MEDIUM	An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31. There is a NULL pointer dereference in work_stuff_copy_to_from when called from iterate_demangle_function.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4803
2116	CVE-2018-17582	MEDIUM	HIGH	Tcpreplay v4.3.0 beta1 contains a heap-based buffer over-read. The get_next_packet() function in the send_packets.c file uses the memcpy() function unsafely to copy sequences from the source buffer pktdata to the destination (*prev_packet)->pktdata. This will result in a Denial of Service (DoS) and potentially Information Exposure when the application attempts to process a file.	tcpreplay	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4794
2117	CVE-2018-17580	MEDIUM	HIGH	A heap-based buffer over-read exists in the function fast_edit_packet() in the file send_packets.c of Tcpreplay v4.3.0 beta1. This can lead to Denial of Service (DoS) and potentially Information Exposure when the application attempts to process a crafted pcap file.	tcpreplay	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4801
2118	CVE-2018-17540	MEDIUM	HIGH	The gmp plugin in strongSwan before 5.7.1 has a Buffer Overflow via a crafted certificate.	strongswan	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4782
2119	CVE-2018-17456	HIGH	CRITICAL	Git before 2.14.5, 2.15.x before 2.15.3, 2.16.x before 2.16.5, 2.17.x before 2.17.2, 2.18.x before 2.18.1, and 2.19.x before 2.19.1 allows remote code execution during processing of a recursive git clone of a superproject if a .gitmodules file has a URL field beginning with a '-' character.	git	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4785
2120	CVE-2018-17360	MEDIUM	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. a heap-based buffer over-read in bfd_getl32 in libbfd.c allows an attacker to cause a denial of service through a crafted PE file. This vulnerability can be triggered by the executable objdump.	binutils	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	10.18.44.2	Not vulnerable	Not vulnerable	LIN10-4792
2121	CVE-2018-17359	MEDIUM	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. An invalid memory access exists in bfd_zalloc in opncls.c. Attackers could leverage this vulnerability to cause a denial of service (application crash) via a crafted ELF file.	binutils	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	10.18.44.2	Not vulnerable	Not vulnerable	LIN10-4823
2122	CVE-2018-17358	MEDIUM	MEDIUM	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31. An invalid memory access exists in _bfd_stab_section_find_nearest_line in syms.c. Attackers could leverage this vulnerability to cause a denial of service (application crash) via a crafted ELF file.	binutils	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	10.18.44.2	Not vulnerable	Not vulnerable	LIN10-4790
2123	CVE-2018-17336	MEDIUM	HIGH	UDisks 2.8.0 has a format string vulnerability in udisks_log in udiskslogging.c, allowing attackers to obtain sensitive information (stack contents), cause a denial of service (memory corruption), or possibly have unspecified other impact via a malformed filesystem label, as demonstrated by %d or %n substrings.	udisks	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4806
2124	CVE-2018-17204	MEDIUM	MEDIUM	An issue was discovered in Open vSwitch (OvS) 2.7.x through 2.7.6, affecting parse_group_prop_ntr_selection_method in lib/ofp-util.c. When decoding a group mod, it validates the group type and command after the whole group mod has been decoded. The OF1.5 decoder, however, tries to use the type and command earlier, when it might still be invalid. This causes an assertion failure (via OVS_NOT_REACHED). ovs-vswitchd does not enable support for OpenFlow 1.5 by default.	openvswitch	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4812
2125	CVE-2018-17199	MEDIUM	HIGH	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.	apache	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3513
2126	CVE-2018-17189	MEDIUM	MEDIUM	In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.	apache	Unchanged	Not vulnerable	Vulnerable	10.17.41.15	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3550
2127	CVE-2018-17183	MEDIUM	HIGH	Artifex Ghostscript before 9.25 allowed a user-writable error exception table, which could be used by remote attackers able to supply crafted PostScript to potentially overwrite or replace error handlers to inject code.	ghostscript	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4786
2128	CVE-2018-17182	HIGH	HIGH	An issue was discovered in the Linux kernel through 4.18.8. The vmacache_flush_all function in mm/vmacache.c mishandles sequence number overflows. An attacker can trigger a use-after-free (and possibly gain privileges) via certain thread creation, map, unmap, invalidation, and dereference operations.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4773
2129	CVE-2018-17101	MEDIUM	HIGH	An issue was discovered in LibTIFF 4.0.9. There are two out-of-bounds writes in cpTags in tools/tiff2bw.c and tools/pal2rgb.c, which can cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image file.	tiff	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4732
2130	CVE-2018-17100	MEDIUM	HIGH	An issue was discovered in LibTIFF 4.0.9. There is a int32 overflow in multiply_ms in tools/ppm2tiff.c, which can cause a denial of service (crash) or possibly have unspecified other impact via a crafted image file.	tiff	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4695

	A	B	C	D	E	F	G	H	I	J	K	L	M
2131	CVE-2018-17082	MEDIUM	MEDIUM	The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a Transfer-Encoding: chunked request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.	php	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4729
2132	CVE-2018-17075	MEDIUM	HIGH	The html package (aka x/net/html) before 2018-07-13 in Go mishandles in frameset insertion mode, leading to a panic: runtime error for html.Parse of <template><object>, <template><applet>, or <template><marquee>. This is related to HTMLTreeBuilder.cpp in WebKit.	go	Unchanged	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4692
2133	CVE-2018-17000	MEDIUM	MEDIUM	A NULL pointer dereference in the function _TIFFmemcmp at tif_unix.c (called from TIFFWriteDirectoryTagTransferfunction) in LibTIFF 4.0.9 allows an attacker to cause a denial-of-service through a crafted tiff file. This vulnerability can be triggered by the executable tiffcp.	tiff	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN10-4693
2134	CVE-2018-16999	MEDIUM	MEDIUM	Netwide Assembler (NASM) 2.14rc15 has an invalid memory write (segmentation fault) in expand_smacro in preproc.c, which allows attackers to cause a denial of service via a crafted input file.	nasm	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.5	Not vulnerable	Not vulnerable	LIN10-4965
2135	CVE-2018-16983	HIGH	CRITICAL	NoScript Classic before 5.1.8.7, as used in Tor Browser 7.x and other products, allows attackers to bypass script blocking via the text/html;/json Content-Type value.	tor	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4680
2136	CVE-2018-16890	Medium	MEDIUM	libcurl versions from 7.36.0 to before 7.64.0 is vulnerable to a heap buffer out-of-bounds read. The function handling incoming NTLM type-2 messages (`lib/vauth/ntlm.c:ntlm_decode_type2_target`) does not validate incoming data correctly and is subject to an integer overflow vulnerability. Using that overflow, a malicious or broken NTLM server could trick libcurl to accept a bad length + offset combination that would lead to a buffer read out-of-bounds.	curl	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3561
2137	CVE-2018-16889	MEDIUM	HIGH	Ceph does not properly sanitize encryption keys in debug logging for v4 auth. This results in the leaking of encryption key information in log files via plaintext	ceph	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3376
2138	CVE-2018-16888	LOW	MEDIUM	It was discovered systemd does not correctly check the content of PIDFile files before using it to kill processes. When a service is run from an unprivileged user (e.g. User field set in the service file), a local attacker who is able to write to the PIDFile of the mentioned service may use this flaw to trick systemd into killing other services and/or privileged processes. Versions before v237 are vulnerable.	systemd	Unchanged	Vulnerable	Vulnerable	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3406
2139	CVE-2018-16886	MEDIUM	HIGH	etcd versions 3.2.x before 3.2.26 and 3.3.x before 3.3.11 are vulnerable to an improper authentication issue when role-based access control (RBAC) is used and client-cert-auth is enabled. If an etcd client server TLS certificate contains a Common Name (CN) which matches a valid RBAC username, a remote attacker may authenticate as that user with any valid (trusted) client certificate in a REST API request to the gRPC-gateway.	etcd	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN1018-3405
2140	CVE-2018-16885	MEDIUM	MEDIUM	A flaw was found in the Linux kernel that allows the userspace to call memcpy_fromiovecend() and similar functions with a zero offset and buffer length which causes the read beyond the buffer boundaries, in certain cases causing a memory access fault and a system halt by accessing invalid memory address. This issue only affects kernel version 3.10.x as shipped with Red Hat Enterprise Linux 7.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3389
2141	CVE-2018-16884	MEDIUM	HIGH	A flaw was found in the Linux kernel in the NFS41+ subsystem. NFS41+ shares mounted in different network namespaces at the same time can make bc_svc_process() use wrong back-channel id and cause a use-after-free. Thus a malicious container user can cause a host kernel memory corruption and a system panic. Due to the nature of the flaw, privilege escalation cannot be fully ruled out.	linux	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.5	Not vulnerable	Vulnerable	LIN1018-3226
2142	CVE-2018-16883	LOW	MEDIUM	sssd versions from 1.13.0 to before 2.0.0 did not properly restrict access to the infopipe according to the allowed_uids configuration parameter. If sensitive information were stored in the user directory, this could be inadvertently disclosed to local attackers.	sssd	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3342
2143	CVE-2018-16882	MEDIUM	HIGH	A use-after-free issue was found in the way the Linux kernel's KVM hypervisor processed posted interrupts when nested(=1) virtualization is enabled. In nested_get_vmcs12_pages(), in case of an error while processing posted interrupt address, it unmaps the 'pi_desc_page' without resetting 'pi_desc' descriptor address, which is later used in pi_test_and_clear_on(). A guest user/process could use this flaw to crash the host kernel resulting in DoS or potentially gain privileged access to a system. Kernel versions before 4.14.91 and before 4.19.13 are vulnerable.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3390
2144	CVE-2018-16881	Medium	HIGH	A denial of service vulnerability was found in rsyslog in the imptcp module. An attacker could send a specially crafted message to the imptcp socket, which would cause rsyslog to crash. Versions before 8.27.0 are vulnerable.	rsyslog	Unchanged	8.0.0.30	9.0.0.20	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3569
2145	CVE-2018-16880	Medium	HIGH	A flaw was found in the Linux kernel's handle_rx() function in the [vhost_net] driver. A malicious virtual guest, under specific conditions, can trigger an out-of-bounds write in a kmalloc-8 slab on a virtual host which may lead to a kernel memory corruption and a system panic. Due to the nature of the flaw, privilege escalation cannot be fully ruled out. Versions from v4.16 and newer are vulnerable.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.5	Not vulnerable	Not vulnerable	LIN1018-3525
2146	CVE-2018-16878	Low	MEDIUM	A flaw was found in pacemaker up to and including version 2.0.1. An insufficient verification inflicted preference of uncontrolled processes can lead to DoS	pacemaker	Unchanged	Vulnerable	Vulnerable	Vulnerable	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3960

	A	B	C	D	E	F	G	H	I	J	K	L	M
2147	CVE-2018-16877	Medium	HIGH	A flaw was found in the way pacemaker's client-server authentication was implemented in versions up to and including 2.0.0. A local attacker could use this flaw, and combine it with other IPC weaknesses, to achieve local privilege escalation.	pacemaker	Unchanged	Vulnerable	Vulnerable	Vulnerable	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3961
2148	CVE-2018-16875	HIGH	HIGH	The crypto/x509 package of Go before 1.10.6 and 1.11.x before 1.11.3 does not limit the amount of work performed for each chain verification, which might allow attackers to craft pathological inputs leading to a CPU denial of service. Go TLS servers accepting client certificates and TLS clients are affected.	go	Unchanged	Not vulnerable	Won't Fix	10.17.41.14	10.18.44.3	10.19.45.1	Not vulnerable	LIN1018-3230
2149	CVE-2018-16874	MEDIUM	HIGH	In Go before 1.10.6 and 1.11.x before 1.11.3, the go get command is vulnerable to directory traversal when executed with the import path of a malicious Go package which contains curly braces (both '{' and '}' characters). Specifically, it is only vulnerable in GOPATH mode, but not in module mode (the distinction is documented at https://golang.org/cmd/go/#hdr-Module_aware_go_get). The attacker can cause an arbitrary filesystem write, which can lead to code execution.	go	Unchanged	Not vulnerable	Won't Fix	10.17.41.14	10.18.44.3	10.19.45.1	Not vulnerable	LIN1018-3201
2150	CVE-2018-16873	MEDIUM	HIGH	In Go before 1.10.6 and 1.11.x before 1.11.3, the go get command is vulnerable to remote code execution when executed with the -u flag and the import path of a malicious Go package, or a package that imports it directly or indirectly. Specifically, it is only vulnerable in GOPATH mode, but not in module mode (the distinction is documented at https://golang.org/cmd/go/#hdr-Module_aware_go_get). Using custom domains, it's possible to arrange things so that a Git repository is cloned to a folder named .git by using a vanity import path that ends with /.git. If the Git repository root contains a HEAD file, a config file, an objects directory, a refs directory, with some work to ensure the proper ordering of operations, go get -u can be tricked into considering the parent directory as a repository root, and running Git commands on it. That will use the config file in the original Git repository root for its configuration, and if that config file contains malicious commands, they will execute on the system running go get -u.	go	Unchanged	Not vulnerable	Won't Fix	10.17.41.14	10.18.44.3	10.19.45.1	Not vulnerable	LIN1018-3249
2151	CVE-2018-16872	LOW	MEDIUM	A flaw was found in qemu Media Transfer Protocol (MTP). The code opening files in usb_mtp_get_object and usb_mtp_get_partial_object and directories in usb_mtp_object_readdir doesn't consider that the underlying filesystem may have changed since the time lstat(2) was called in usb_mtp_object_alloc, a classical TOCTTOU problem. An attacker with write access to the host filesystem shared with a guest can use this property to navigate the host filesystem in the context of the QEMU process and read any file the QEMU process has access to. Access to the filesystem may be local or via a network share protocol such as CIFS.	qemu	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	10.19.45.1	Not vulnerable	LIN1018-3242
2152	CVE-2018-16871	MEDIUM	HIGH	A flaw was found in the Linux kernel's NFS implementation, all versions 3.x and all versions 4.x up to 4.20. An attacker, who is able to mount an exported NFS filesystem, is able to trigger a null pointer dereference by using an invalid NFS sequence. This can panic the machine and deny access to the NFS server. Any outstanding disk writes to the NFS server will be lost.	linux	Unchanged	Not vulnerable	9.0.0.22	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4573
2153	CVE-2018-16870	MEDIUM	MEDIUM	It was found that wolfssl before 3.15.7 is vulnerable to a new variant of the Bleichenbacher attack to perform downgrade attacks against TLS. This may lead to leakage of sensible data.	wolfssl	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3416
2154	CVE-2018-16869	LOW	MEDIUM	A Bleichenbacher type side-channel based padding oracle attack was found in the way nettle handles endian conversion of RSA decrypted PKCS#1 v1.5 data. An attacker who is able to run a process on the same physical core as the victim process, could use this flaw extract plaintext or in some cases downgrade any TLS connections to a vulnerable server.	nettle	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3197
2155	CVE-2018-16868	LOW	MEDIUM	A Bleichenbacher type side-channel based padding oracle attack was found in the way gnutls handles verification of RSA decrypted PKCS#1 v1.5 data. An attacker who is able to run process on the same physical core as the victim process, could use this to extract plaintext or in some cases downgrade any TLS connections to a vulnerable server.	gnutls	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3200
2156	CVE-2018-16867	MEDIUM	HIGH	A flaw was found in qemu Media Transfer Protocol (MTP) before version 3.1.0. A path traversal in the in usb_mtp_write_data function in hw/usb/dev-mtp.c due to an improper filename sanitization. When the guest device is mounted in read-write mode, this allows to read/write arbitrary files which may lead do DoS scenario OR possibly lead to code execution on the host.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3257
2157	CVE-2018-16866	LOW	LOW	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.	systemd	Unchanged	8.0.0.30	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3408
2158	CVE-2018-16865	MEDIUM	HIGH	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.	systemd	Unchanged	8.0.0.30	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3379

	A	B	C	D	E	F	G	H	I	J	K	L	M
2159	CVE-2018-16864	MEDIUM	HIGH	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.	systemd	Unchanged	8.0.0.30	9.0.0.20	10.17.41.14	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3404
2160	CVE-2018-16863	HIGH	HIGH	It was found that RHSA-2018:2918 did not fully fix CVE-2018-16509. An attacker could possibly exploit another variant of the flaw and bypass the -dSAFER protection to, for example, execute arbitrary shell commands via a specially crafted PostScript document. This only affects ghostscript 9.07 as shipped with Red Hat Enterprise Linux 7.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3213
2161	CVE-2018-16862	LOW	MEDIUM	A security flaw was found in the Linux kernel in a way that the cleancache subsystem clears an inode after the final file truncation (removal). The new file created with the same inode may contain leftover pages from cleancache and so the old file data instead of the new one.	linux	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.5	Not vulnerable	Not vulnerable	LIN10-5058
2162	CVE-2018-16860	Medium	HIGH	A flaw was found in samba's Heimdal KDC implementation, versions 4.8.x up to, excluding 4.8.12, 4.9.x up to, excluding 4.9.8 and 4.10.x up to, excluding 4.10.3, when used in AD DC mode. A man in the middle attacker could use this flaw to intercept the request to the KDC and replace the user name (principal) in the request with any desired user name (principal) that exists in the KDC effectively obtaining a ticket for that principal.	samba	Unchanged	Not vulnerable	Not vulnerable	10.17.41.17	10.18.44.10	Not vulnerable	Not vulnerable	LIN1018-4596
2163	CVE-2018-16857	MEDIUM	MEDIUM	Samba from version 4.9.0 and before version 4.9.3 that have AD DC configurations watching for bad passwords (to restrict brute forcing of passwords) in a window of more than 3 minutes may not watch for bad passwords at all. The primary risk from this issue is with regards to domains that have been upgraded from Samba 4.8 and earlier. In these cases the manual testing done to confirm an organisation's password policies apply as expected may not have been re-done after the upgrade.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3254
2164	CVE-2018-16853	MEDIUM	MEDIUM	Samba from version 4.7.0 has a vulnerability that allows a user in a Samba AD domain to crash the KDC when Samba is built in the non-default MIT Kerberos configuration. With this advisory the Samba Team clarify that the MIT Kerberos build of the Samba AD DC is considered experimental. Therefore the Samba Team will not issue security patches for this configuration. Additionally, Samba 4.7.12, 4.8.7 and 4.9.3 have been issued as security releases to prevent building of the AD DC with MIT Kerberos unless --with-experimental-mit-ad-dc is specified to the configure command.	samba	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3244
2165	CVE-2018-16852	LOW	MEDIUM	Samba from version 4.9.0 and before version 4.9.3 is vulnerable to a NULL pointer de-reference. During the processing of an DNS zone in the DNS management DCE/RPC server, the internal DNS server or the Samba DLZ plugin for BIND9, if the DSPROPERTY_ZONE_MASTER_SERVERS property or DSPROPERTY_ZONE_SCAVENGING_SERVERS property is set, the server will follow a NULL pointer and terminate. There is no further vulnerability associated with this issue, merely a denial of service.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3238
2166	CVE-2018-16851	MEDIUM	MEDIUM	Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.	samba	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3245
2167	CVE-2018-16850	HIGH	CRITICAL	postgresql before versions 11.1, 10.6 is vulnerable to a to SQL injection in pg_upgrade and pg_dump via CREATE TRIGGER ... REFERENCING. Using a purpose-crafted trigger definition, an attacker can cause arbitrary SQL statements to run, with superuser privileges.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-5013
2168	CVE-2018-16847	MEDIUM	HIGH	An OOB heap buffer r/w access issue was found in the NVM Express Controller emulation in QEMU. It could occur in nvme_cmb_ops routines in nvme device. A guest user/process could use this flaw to crash the QEMU process resulting in DoS or potentially run arbitrary code with privileges of the QEMU process.	qemu	Unchanged	Not vulnerable	Not vulnerable	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4991
2169	CVE-2018-16846	MEDIUM	MEDIUM	ceph: ListBucket max-keys has no defined limit in the RGW codebase	ceph	Unchanged	8.0.0.30	9.0.0.20	Won't Fix	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3385
2170	CVE-2018-16845	MEDIUM	MEDIUM	nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.	nginx	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5007
2171	CVE-2018-16844	HIGH	HIGH	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.	nginx	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5008

	A	B	C	D	E	F	G	H	I	J	K	L	M
2172	CVE-2018-16843	HIGH	HIGH	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.	nginx	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4980
2173	CVE-2018-16842	MEDIUM	CRITICAL	curl contains a heap out of buffer read vulnerability. The command line tool has a generic function for displaying warning and informational messages to stderr for various situations. For example if an unknown command line argument is used, or passed to it in a "config" file. This display function formats the output to wrap at 80 columns. The wrap logic is however flawed, so if a single word in the message is itself longer than 80 bytes the buffer arithmetic calculates the remainder wrong and will end up reading behind the end of the buffer. This could lead to information disclosure or crash.	curl	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4867
2174	CVE-2018-16841	MEDIUM	MEDIUM	Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.	samba	Unchanged	Not vulnerable	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3261
2175	CVE-2018-16840	HIGH	CRITICAL	libcurl contains a heap use-after-free flaw in code related to closing an easy handle. When closing and cleaning up an "easy" handle in the Curl_close() function, the library code first frees a struct (without nulling the pointer) and might then subsequently erroneously write to a struct field within that already freed struct.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4887
2176	CVE-2018-16839	HIGH	CRITICAL	libcurl contains a buffer overrun in the SASL authentication code. The internal function Curl_auth_create_plain_message fails to correctly verify that the passed in lengths for name and password aren't too long, then calculates a buffer size to allocate. On systems with a 32 bit size_t, the math to calculate the buffer size triggers an integer overflow when the user name length exceeds 2GB (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the intended very huge one, making the use of that buffer end up in a heap buffer overflow.	curl	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4881
2177	CVE-2018-16838	MEDIUM	MEDIUM	A flaw was found in sssd Group Policy Objects implementation. When the GPO is not readable by SSSD due to a too strict permission settings on the server side, SSSD will allow all authenticated users to login instead of denying access.	sssd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	10.18.44.15	10.19.45.6	Won't Fix	LIN1018-3799
2178	CVE-2018-16802	MEDIUM	HIGH	An issue was discovered in Artifex Ghostscript before 9.25. Incorrect restoration of privilege checking when running out of stack during exception handling could be used by attackers able to supply crafted PostScript to execute code using the pipe instruction. This is due to an incomplete fix for CVE-2018-16509.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4703
2179	CVE-2018-16790	MEDIUM	HIGH	_bson_iter_next_internal in bson-iter.c in libbson 1.12.0, as used in MongoDB mongo-c-driver and other products, has a heap-based buffer over-read via a crafted bson buffer.	mongodb	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4684
2180	CVE-2018-16750	MEDIUM	MEDIUM	In ImageMagick 7.0.7-29 and earlier, a memory leak in the formatIPTCfromBuffer function in coders/meta.c was found.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4711
2181	CVE-2018-16749	MEDIUM	MEDIUM	In ImageMagick 7.0.7-29 and earlier, a missing NULL check in ReadOneJNGImage in coders/png.c allows an attacker to cause a denial of service (WriteBlob assertion failure and application exit) via a crafted file.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4672
2182	CVE-2018-16658	LOW	MEDIUM	An issue was discovered in the Linux kernel before 4.18.6. An information leak in cdrom_ioctl_drive_status in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4700
2183	CVE-2018-16646	MEDIUM	MEDIUM	In Poppler 0.68.0, the Parser::getObj() function in Parser.cc may cause infinite recursion via a crafted file. A remote attacker can leverage this for a DoS attack.	poppler	Unchanged	Won't Fix	9.0.0.22	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4738
2184	CVE-2018-16645	MEDIUM	MEDIUM	There is an excessive memory allocation issue in the functions ReadBMPImage of coders/bmp.c and ReadDIBImage of coders/dib.c in ImageMagick 7.0.8-11, which allows remote attackers to cause a denial of service via a crafted image file.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4716
2185	CVE-2018-16644	MEDIUM	MEDIUM	There is a missing check for length in the functions ReadDCMImage of coders/dcm.c and ReadPICTImage of coders/pict.c in ImageMagick 7.0.8-11, which allows remote attackers to cause a denial of service via a crafted image.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4683
2186	CVE-2018-16643	MEDIUM	MEDIUM	The functions ReadDCMImage in coders/dcm.c, ReadPWPImage in coders/pwp.c, ReadCALSImage in coders/cals.c, and ReadPICTImage in coders/pict.c in ImageMagick 7.0.8-4 do not check the return value of the fputc function, which allows remote attackers to cause a denial of service via a crafted image file.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4707
2187	CVE-2018-16642	MEDIUM	MEDIUM	The function InsertRow in coders/cut.c in ImageMagick 7.0.7-37 allows remote attackers to cause a denial of service via a crafted image file due to an out-of-bounds write.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4686
2188	CVE-2018-16641	MEDIUM	MEDIUM	ImageMagick 7.0.8-6 has a memory leak vulnerability in the TIFFWritePhotoshopLayers function in coders/tiff.c.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4714
2189	CVE-2018-16640	MEDIUM	MEDIUM	ImageMagick 7.0.8-5 has a memory leak vulnerability in the function ReadOneJNGImage in coders/png.c.	imagemagick	Unchanged	8.0.0.28	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4691

	A	B	C	D	E	F	G	H	I	J	K	L	M
2190	CVE-2018-16597	MEDIUM	MEDIUM	An issue was discovered in the Linux kernel through 4.18.6. Incorrect access checking in overlayfs mounts could be used by local attackers to modify or truncate files in the underlying filesystem.	linux	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4774
2191	CVE-2018-16585	MEDIUM	HIGH	An issue was discovered in Artifex Ghostscript before 9.24. The .setdistillerkeys PostScript command is accepted even though it is not intended for use during document processing (e.g., after the startup phase). This leads to memory corruption, allowing remote attackers able to supply crafted PostScript to crash the interpreter or possibly have unspecified other impact.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4675
2192	CVE-2018-16543	MEDIUM	HIGH	In Artifex Ghostscript before 9.24, gssetresolution and gsgetresolution allow attackers to have an unspecified impact.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4743
2193	CVE-2018-16542	MEDIUM	MEDIUM	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use insufficient interpreter stack-size checking during error handling to crash the interpreter.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4731
2194	CVE-2018-16541	MEDIUM	MEDIUM	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use incorrect free logic in pagedevice replacement to crash the interpreter.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4734
2195	CVE-2018-16540	MEDIUM	HIGH	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files to the builtin PDF14 converter could use a use-after-free in copydevice handling to crash the interpreter or possibly have unspecified other impact.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4718
2196	CVE-2018-16539	MEDIUM	MEDIUM	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use incorrect access checking in temp file handling to disclose contents of files on the system otherwise not readable.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4737
2197	CVE-2018-16513	MEDIUM	HIGH	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use a type confusion in the setcolor function to crash the interpreter or possibly have unspecified other impact.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4745
2198	CVE-2018-16511	MEDIUM	HIGH	An issue was discovered in Artifex Ghostscript before 9.24. A type confusion in ztype could be used by remote attackers able to supply crafted PostScript to crash the interpreter or possibly have unspecified other impact.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4702
2199	CVE-2018-16510	MEDIUM	HIGH	An issue was discovered in Artifex Ghostscript before 9.24. Incorrect exec stack handling in the CS and SC PDF primitives could be used by remote attackers able to supply crafted PDFs to crash the interpreter or possibly have unspecified other impact.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4704
2200	CVE-2018-16509	HIGH	HIGH	An issue was discovered in Artifex Ghostscript before 9.24. Incorrect restoration of privilege checking during handling of /invalidaccess exceptions could be used by attackers able to supply crafted PostScript to execute code using the pipe instruction.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4742
2201	CVE-2018-16471	MEDIUM	MEDIUM	There is a possible XSS vulnerability in Rack before 2.0.6 and 1.6.11. Carefully crafted requests can impact the data returned by the `scheme` method on `Rack::Request`. Applications that expect the scheme to be limited to 'http' or 'https' and do not escape the return value could be vulnerable to an XSS attack. Note that applications using the normal escaping mechanisms provided by Rails may not impacted, but applications that bypass the escaping mechanisms, or do not use them may be vulnerable.	rack	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-5020
2202	CVE-2018-16470	MEDIUM	HIGH	There is a possible DoS vulnerability in the multipart parser in Rack before 2.0.6. Specially crafted requests can cause the multipart parser to enter a pathological state, causing the parser to use CPU resources disproportionate to the request size.	rack	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4990
2203	CVE-2018-16452	Medium	HIGH	The SMB parser in tcpdump before 4.9.3 has stack exhaustion in smbutil.c:smb_fdata() via recursion.	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-5002
2204	CVE-2018-16451	High	CRITICAL	The SMB parser in tcpdump before 4.9.3 has buffer over-reads in print-smb.c:print_trans() for \MAILSLOT\BROWSE and \PIPE\LANMAN.	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-5001
2205	CVE-2018-16427	LOW	MEDIUM	Various out of bounds reads when handling responses in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to potentially crash the opensc library using programs.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4726
2206	CVE-2018-16426	LOW	MEDIUM	Endless recursion when handling responses from an IAS-ECC card in iasecc_select_file in libopensc/card-iasecc.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to hang or crash the opensc library using programs.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4723
2207	CVE-2018-16425	MEDIUM	MEDIUM	A double free when handling responses from an HSM Card in sc_pkcs15emu_sc_hsm_init in libopensc/pkcs15-sc-hsm.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4727
2208	CVE-2018-16424	MEDIUM	MEDIUM	A double free when handling responses in read_file in tools/egk-tool.c (aka the eGK card tool) in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4715
2209	CVE-2018-16423	MEDIUM	MEDIUM	A double free when handling responses from a smartcard in sc_file_set_sec_attr in libopensc/sc.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4733
2210	CVE-2018-16422	MEDIUM	MEDIUM	A single byte buffer overflow when handling responses from an esteid Card in sc_pkcs15emu_esteid_init in libopensc/pkcs15-esteid.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4722

	A	B	C	D	E	F	G	H	I	J	K	L	M
2211	CVE-2018-16421	MEDIUM	MEDIUM	Several buffer overflows when handling responses from a CAC Card in cac_get_serial_nr_from_CUID in libopensc/card-cac.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4685
2212	CVE-2018-16420	MEDIUM	MEDIUM	Several buffer overflows when handling responses from an ePass 2003 Card in decrypt_response in libopensc/card-epass2003.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4696
2213	CVE-2018-16419	MEDIUM	MEDIUM	Several buffer overflows when handling responses from a Cryptoflex card in read_public_key in tools/cryptoflex-tool.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4678
2214	CVE-2018-16418	MEDIUM	MEDIUM	A buffer overflow when handling string concatenation in util_acl_to_str in tools/util.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4739
2215	CVE-2018-16413	MEDIUM	HIGH	ImageMagick 7.0.8-11 Q16 has a heap-based buffer over-read in the MagickCore/quantum-private.h PushShortPixel function when called from the coders/psd.c ParseImageResourceBlocks function.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4673
2216	CVE-2018-16412	MEDIUM	HIGH	ImageMagick 7.0.8-11 Q16 has a heap-based buffer over-read in the coders/psd.c ParseImageResourceBlocks function.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4706
2217	CVE-2018-16403	MEDIUM	MEDIUM	libdw in elfutils 0.173 checks the end of the attributes list incorrectly in dwarf_getabbrev in dwarf_getabbrev.c and dwarf_hasattr in dwarf_hasattr.c, leading to a heap-based buffer over-read and an application crash.	elfutils	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4720
2218	CVE-2018-16402	HIGH	CRITICAL	libelf/elf_end.c in elfutils 0.173 allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact because it tries to decompress twice.	elfutils	Unchanged	Not vulnerable	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4676
2219	CVE-2018-16396	MEDIUM	HIGH	Array#pack method converts the receiver's contents into a string with specified format. If the receiver contains some tainted objects, the returned string also should be tainted. String#unpack method which converts the receiver into an array also should propagate its tainted flag to the objects contained in the returned array. But, with B, b, H and h directives, the tainted flags are not propagated. So, if a script processes unreliable inputs by Array#pack and/or String#unpack with these directives and checks the reliability with tainted flags, the check might be wrong.	ruby	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4995
2220	CVE-2018-16395	HIGH	CRITICAL	An instance of OpenSSL::X509::Name contains entities such as CN, C and so on. Some two instances of OpenSSL::X509::Name are equal only when all entities are exactly equal. However, there is a bug that the equality check is not correct if the value of an entity of the argument (right-hand side) starts with the value of the receiver (left-hand side). So, if a malicious X.509 certificate is passed to compare with an existing certificate, there is a possibility to be judged incorrectly that they are equal.	ruby	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4998
2221	CVE-2018-16393	MEDIUM	MEDIUM	Several buffer overflows when handling responses from a Gemsafe V1 Smartcard in gemsafe_get_cert_len in libopensc/pkcs15-gemsafeV1.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4744
2222	CVE-2018-16392	MEDIUM	MEDIUM	Several buffer overflows when handling responses from a TCOS Card in tcos_select_file in libopensc/card-tcos.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4690
2223	CVE-2018-16391	MEDIUM	MEDIUM	Several buffer overflows when handling responses from a Muscle Card in muscle_list_files in libopensc/card-muscle.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.	opensc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4724
2224	CVE-2018-16376	MEDIUM	HIGH	An issue was discovered in OpenJPEG 2.3.0. A heap-based buffer overflow was discovered in the function t2_encode_packet in lib/openmj2/t2.c. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly unspecified other impact.	openjpeg	Unchanged	Won't Fix	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4725
2225	CVE-2018-16375	MEDIUM	HIGH	An issue was discovered in OpenJPEG 2.3.0. Missing checks for header_info.height and header_info.width in the function pnmtoimage in bin/jpwl/convert.c can lead to a heap-based buffer overflow.	openjpeg	Unchanged	Won't Fix	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4719
2226	CVE-2018-16335	MEDIUM	HIGH	newoffsets handling in ChopUpSingleUncompressedStrip in tif_dirread.c in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted TIFF file, as demonstrated by tiff2pdf. This is a different vulnerability than CVE-2018-15209.	tiff	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4681
2227	CVE-2018-16329	HIGH	CRITICAL	In ImageMagick before 7.0.8-8, a NULL pointer dereference exists in the GetMagickProperty function in MagickCore/property.c.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4687
2228	CVE-2018-16328	HIGH	CRITICAL	In ImageMagick before 7.0.8-8, a NULL pointer dereference exists in the CheckEventLogging function in MagickCore/log.c.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4688

	A	B	C	D	E	F	G	H	I	J	K	L	M
2229	CVE-2018-16323	MEDIUM	MEDIUM	ReadXBMImage in coders/xbm.c in ImageMagick before 7.0.8-9 leaves data uninitialized when processing an XBM file that has a negative pixel value. If the affected code is used as a library loaded into a process that includes sensitive information, that information sometimes can be leaked via the image data.	imagemagick	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4730
2230	CVE-2018-16301	High	CRITICAL	libpcap before 1.9.1, as used in tcpdump before 4.9.3, has a buffer overflow and/or over-read because of errors in pcapng reading.	libpcap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	Not vulnerable	Not vulnerable	LIN1018-5003
2231	CVE-2018-16300	Medium	HIGH	The BGP parser in tcpdump before 4.9.3 allows stack consumption in print-bgp.c:bgp_attr_print() because of unlimited recursion.	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-5000
2232	CVE-2018-16276	HIGH	HIGH	An issue was discovered in yurex_read in drivers/usb/misc/yurex.c in the Linux kernel before 4.17.7. Local attackers could use user access read/writes with incorrect bounds checking in the yurex USB driver to crash the kernel or potentially escalate privileges.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4735
2233	CVE-2018-16230	High	CRITICAL	The BGP parser in tcpdump before 4.9.3 has a buffer over-read in print-bgp.c:bgp_attr_print() (MP_REACH_NLRI).	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4999
2234	CVE-2018-16229	High	CRITICAL	The DCCP parser in tcpdump before 4.9.3 has a buffer over-read in print-dccp.c:dccp_print_option().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4998
2235	CVE-2018-16228	High	CRITICAL	The HNCP parser in tcpdump before 4.9.3 has a buffer over-read in print-hncp.c:print_prefix().	tcpdump	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4997
2236	CVE-2018-16227	High	CRITICAL	The IEEE 802.11 parser in tcpdump before 4.9.3 has a buffer over-read in print-802_11.c for the Mesh Flags subfield.	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4996
2237	CVE-2018-16152	MEDIUM	HIGH	In verify_emsa_pkcs1_signature() in gmp_rsa_public_key.c in the gmp plugin in strongSwan 4.x and 5.x before 5.7.0, the RSA implementation based on GMP does not reject excess data in the digestAlgorithm.parameters field during PKCS#1 v1.5 signature verification. Consequently, a remote attacker can forge signatures when small public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication. This is a variant of CVE-2006-4790 and CVE-2014-1568.	strongswan	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4800
2238	CVE-2018-16151	MEDIUM	HIGH	In verify_emsa_pkcs1_signature() in gmp_rsa_public_key.c in the gmp plugin in strongSwan 4.x and 5.x before 5.7.0, the RSA implementation based on GMP does not reject excess data after the encoded algorithm OID during PKCS#1 v1.5 signature verification. Similar to the flaw in the same version of strongSwan regarding digestAlgorithm.parameters, a remote attacker can forge signatures when small public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication.	strongswan	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4793
2239	CVE-2018-16062	MEDIUM	MEDIUM	dwarf_getaranges in dwarf_getaranges.c in libdw in elfutils before 2018-08-18 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file.	elfutils	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4596
2240	CVE-2018-16058	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.2, 2.4.0 to 2.4.8, and 2.2.0 to 2.2.16, the Bluetooth AVDTP dissector could crash. This was addressed in epan/dissectors/packet-btavdtp.c by properly initializing a data structure.	wireshark	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4615
2241	CVE-2018-16057	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.2, 2.4.0 to 2.4.8, and 2.2.0 to 2.2.16, the Radiotap dissector could crash. This was addressed in epan/dissectors/packet-ieee80211-radiotap-iter.c by validating iterator operations.	wireshark	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4602
2242	CVE-2018-16056	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.2, 2.4.0 to 2.4.8, and 2.2.0 to 2.2.16, the Bluetooth Attribute Protocol dissector could crash. This was addressed in epan/dissectors/packet-btatt.c by verifying that a dissector for a specific UUID exists.	wireshark	Unchanged	Not vulnerable	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4627
2243	CVE-2018-15919	MEDIUM	MEDIUM	Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or oracle) as a vulnerability.'	openssh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN10-4616
2244	CVE-2018-15911	MEDIUM	HIGH	In Artifex Ghostscript 9.23 before 2018-08-24, attackers able to supply crafted PostScript could use uninitialized memory access in the aesdecode operator to crash the interpreter or potentially execute code.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4633
2245	CVE-2018-15910	MEDIUM	HIGH	In Artifex Ghostscript 9.23 before 2018-08-23, attackers able to supply crafted PostScript files could use a type confusion in the LockDistillerParams parameter to crash the interpreter or execute code.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4638
2246	CVE-2018-15909	MEDIUM	HIGH	In Artifex Ghostscript 9.23 before 2018-08-24, a type confusion using the .shfill operator could be used by attackers able to supply crafted PostScript files to crash the interpreter or potentially execute code.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4609
2247	CVE-2018-15908	MEDIUM	HIGH	In Artifex Ghostscript 9.23 before 2018-08-23, attackers are able to supply malicious PostScript files to bypass .tempfile restrictions and write files.	ghostscript	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4599
2248	CVE-2018-15864	LOW	MEDIUM	Unchecked NULL pointer usage in resolve_keysym in xkbcomp/parser.y in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because a map access attempt can occur for a map that was never created.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4624
2249	CVE-2018-15863	LOW	MEDIUM	Unchecked NULL pointer usage in ResolveStateAndPredicate in xkbcomp/compat.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file with a no-op modmask expression.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4611

	A	B	C	D	E	F	G	H	I	J	K	L	M
2250	CVE-2018-15862	LOW	MEDIUM	Unchecked NULL pointer usage in LookupModMask in xkbcomp/expr.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file with invalid virtual modifiers.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4623
2251	CVE-2018-15861	LOW	MEDIUM	Unchecked NULL pointer usage in ExprResolveLhs in xkbcomp/expr.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file that triggers an xkb_intern_atom failure.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4594
2252	CVE-2018-15859	LOW	MEDIUM	Unchecked NULL pointer usage when parsing invalid atoms in ExprResolveLhs in xkbcomp/expr.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because lookup failures are mishandled.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4598
2253	CVE-2018-15858	LOW	MEDIUM	Unchecked NULL pointer usage when handling invalid aliases in CopyKeyAliasesToKeymap in xkbcomp/keycodes.c in xkbcommon before 0.8.1 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4606
2254	CVE-2018-15857	MEDIUM	HIGH	An invalid free in ExprAppendMultiKeysymList in xkbcomp/ast-build.c in xkbcommon before 0.8.1 could be used by local attackers to crash xkbcommon keymap parsers or possibly have unspecified other impact by supplying a crafted keymap file.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4587
2255	CVE-2018-15856	LOW	MEDIUM	An infinite loop when reaching EOL unexpectedly in compose/parser.c (aka the keymap parser) in xkbcommon before 0.8.1 could be used by local attackers to cause a denial of service during parsing of crafted keymap files.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4608
2256	CVE-2018-15855	LOW	MEDIUM	Unchecked NULL pointer usage in xkbcommon before 0.8.1 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because the XkbFile for an xkb_geometry section was mishandled.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4620
2257	CVE-2018-15854	LOW	MEDIUM	Unchecked NULL pointer usage in xkbcommon before 0.8.1 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because geometry tokens were desupported incorrectly.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4604
2258	CVE-2018-15853	LOW	MEDIUM	Endless recursion exists in xkbcomp/expr.c in xkbcommon and libxkbcommon before 0.8.1, which could be used by local attackers to crash xkbcommon users by supplying a crafted keymap file that triggers boolean negation.	libxkbcommon	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4636
2259	CVE-2018-15822	MEDIUM	HIGH	The flv_write_packet function in libavformat/flvenc.c in FFmpeg through 4.0.2 does not check for an empty audio packet, leading to an assertion failure.	ffmpeg	Unchanged	Not vulnerable	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4614
2260	CVE-2018-15751	HIGH	CRITICAL	SaltStack Salt before 2017.7.8 and 2018.3.x before 2018.3.3 allow remote attackers to bypass authentication and execute arbitrary commands via salt-api(netapi).	salt	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4906
2261	CVE-2018-15750	MEDIUM	MEDIUM	Directory Traversal vulnerability in salt-api in SaltStack Salt before 2017.7.8 and 2018.3.x before 2018.3.3 allows remote attackers to determine which files exist on the server.	salt	Unchanged	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4895
2262	CVE-2018-15746	LOW	MEDIUM	qemu-seccomp.c in QEMU might allow local OS guest users to cause a denial of service (guest crash) by leveraging mishandling of the seccomp policy for threads other than the main thread.	qemu	Unchanged	Not vulnerable	9.0.0.19	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4588
2263	CVE-2018-15688	HIGH	CRITICAL	A buffer overflow vulnerability in the dhcp6 client of systemd allows a malicious dhcp6 server to overwrite heap memory in systemd-networkd. Affected releases are systemd: versions up to and including 239.	systemd	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4901
2264	CVE-2018-15687	LOW	MEDIUM	A race condition in chown_one() of systemd allows an attacker to cause systemd to set arbitrary permissions on arbitrary files. Affected releases are systemd versions up to and including 239.	systemd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4931
2265	CVE-2018-15686	HIGH	CRITICAL	A vulnerability in unit_deserialize of systemd allows an attacker to supply arbitrary state across systemd re-execution via NotifyAccess. This can be used to improperly influence systemd execution and possibly lead to root privilege escalation. Affected releases are systemd versions up to and including 239.	systemd	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	10.19.45.1	Not vulnerable	LIN10-4874
2266	CVE-2018-15664	Medium	HIGH	In Docker through 18.06.1-ce-rc2, the API endpoints behind the 'docker cp' command are vulnerable to a symlink-exchange attack with Directory Traversal, giving attackers arbitrary read-write access to the host filesystem with root privileges, because daemon/archive.go does not do archive operations on a frozen filesystem (or from within a chroot).	docker	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-4151
2267	CVE-2018-15607	HIGH	MEDIUM	In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x36 0x36 0x36 0x36 0x36 0x36 0x1f 0x35 0x50 0x00 can result in a hang of several minutes during which CPU and memory resources are consumed until ultimately an attempted large memory allocation fails. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4632
2268	CVE-2018-15605	MEDIUM	MEDIUM	An issue was discovered in phpMyAdmin before 4.8.3. A Cross-Site Scripting vulnerability has been found where an attacker can use a crafted file to manipulate an authenticated user who loads that file through the import feature.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4592
2269	CVE-2018-15599	MEDIUM	MEDIUM	The recv_msg_userauth_request function in svr-auth.c in Dropbear through 2018.76 is prone to a user enumeration vulnerability because username validity affects how fields in SSH_MSG_USERAUTH messages are handled, a similar issue to CVE-2018-15473 in an unrelated codebase.	dropbear	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4600

	A	B	C	D	E	F	G	H	I	J	K	L	M
2270	CVE-2018-15594	LOW	MEDIUM	arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it easier for attackers to conduct Spectre-v2 attacks against paravirtual guests.	linux	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4621
2271	CVE-2018-15572	LOW	MEDIUM	The spectre_v2_select_mitigation function in arch/x86/kernel/cpu/bugs.c in the Linux kernel before 4.18.1 does not always fill RSB upon a context switch, which makes it easier for attackers to conduct userspace-userspace spectreRSB attacks.	linux	Unchanged	8.0.0.30	9.0.0.18	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4575
2272	CVE-2018-15501	MEDIUM	HIGH	In ng_pkt in transports/smart_pkt.c in libgit2 before 0.26.6 and 0.27.x before 0.27.4, a remote attacker can send a crafted smart-protocol ng packet that lacks a '\0' byte to trigger an out-of-bounds read that leads to DoS.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4589
2273	CVE-2018-15473	MEDIUM	MEDIUM	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.	openssh	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4625
2274	CVE-2018-15471	MEDIUM	HIGH	An issue was discovered in xenvif_set_hash_mapping in drivers/net/xen-netback/hash.c in the Linux kernel through 4.18.1, as used in Xen through 4.11.x and other products. The Linux netback driver allows frontends to control mapping of requests to request queues. When processing a request to set or change this mapping, some input validation (e.g., for an integer overflow) was missing or flawed, leading to OOB access in hash handling. A malicious or buggy frontend may cause the (usually privileged) backend to make out of bounds memory accesses, potentially resulting in one or more of privilege escalation, Denial of Service (DoS), or information leaks.	linux	Unchanged	Not vulnerable	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4603
2275	CVE-2018-15378	MEDIUM	MEDIUM	A vulnerability in ClamAV versions prior to 0.100.2 could allow an attacker to cause a denial of service (DoS) condition. The vulnerability is due to an error related to the MEW unpacker within the unmew11() function (libclamav/mew.c), which can be exploited to trigger an invalid read memory access via a specially crafted EXE file.	clamav	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4919
2276	CVE-2018-15209	MEDIUM	HIGH	ChopUpSingleUncompressedStrip in tif_dirread.c in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted TIFF file, as demonstrated by tiff2pdf.	tiff	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4526
2277	CVE-2018-15173	MEDIUM	HIGH	Nmap through 7.70, when the -sV option is used, allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted TCP-based service.	nmap	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN10-4543
2278	CVE-2018-15127	HIGH	CRITICAL	LibVNC before commit 502821828ed00b4a2c4bef90683d0fd88ce495de contains heap out-of-bound write vulnerability in server code of file transfer extension that can result remote code execution	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3293
2279	CVE-2018-15126	HIGH	CRITICAL	LibVNC before commit 73cb96fec028a576a5a24417b57723b55854ad7b contains heap use-after-free vulnerability in server code of file transfer extension that can result remote code execution	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3306
2280	CVE-2018-15120	MEDIUM	HIGH	libpango in Pango before 1.42.4, as used in hexchat and other products, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted text.	pango	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4630
2281	CVE-2018-14884	MEDIUM	HIGH	An issue was discovered in PHP 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1. Inappropriately parsing an HTTP response leads to a segmentation fault because http_header_value in ext/standard/http_fopen_wrapper.c can be a NULL value that is mishandled in an atoi call.	php	Unchanged	Not vulnerable	Not vulnerable	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4549
2282	CVE-2018-14883	MEDIUM	HIGH	An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.	php	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4527
2283	CVE-2018-14882	High	CRITICAL	The ICMPv6 parser in tcpdump before 4.9.3 has a buffer over-read in print-icmp6.c.	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4995
2284	CVE-2018-14881	High	CRITICAL	The BGP parser in tcpdump before 4.9.3 has a buffer over-read in print-bgp.c:bgp_capabilities_print() (BGP_CAPCODE_RESTART).	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4994
2285	CVE-2018-14880	High	CRITICAL	The OSPFv3 parser in tcpdump before 4.9.3 has a buffer over-read in print-ospf6.c:ospf6_print_lshdr().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4993
2286	CVE-2018-14879	High	CRITICAL	The command-line argument parser in tcpdump before 4.9.3 has a buffer overflow in tcpdump.c:get_next_file().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4992
2287	CVE-2018-14851	MEDIUM	MEDIUM	exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.	php	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4534
2288	CVE-2018-14734	MEDIUM	HIGH	drivers/infiniband/core/ucma.c in the Linux kernel through 4.17.11 allows ucma_leave_multicast to access a certain data structure after a cleanup step in ucma_process_join, which allows attackers to cause a denial of service (use-after-free).	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4465
2289	CVE-2018-14682	MEDIUM	HIGH	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. There is an off-by-one error in the TOLOWER() macro for CHM decompression.	libmspack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4374
2290	CVE-2018-14681	MEDIUM	HIGH	An issue was discovered in kwajd_read_headers in mspack/kwajd.c in libmspack before 0.7alpha. Bad KWAJ file header extensions could cause a one or two byte overwrite.	libmspack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4379
2291	CVE-2018-14680	MEDIUM	MEDIUM	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. It does not reject blank CHM filenames.	libmspack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4414

	A	B	C	D	E	F	G	H	I	J	K	L	M
2292	CVE-2018-14679	MEDIUM	MEDIUM	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. There is an off-by-one error in the CHM PMGI/PMGL chunk number validity checks, which could lead to denial of service (uninitialized data dereference and application crash).	libmspack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4394
2293	CVE-2018-14678	HIGH	HIGH	An issue was discovered in the Linux kernel through 4.17.11, as used in Xen through 4.11.x. The xen_failsafe_callback entry point in arch/x86/entry/entry_64.S does not properly maintain RBX, which allows local users to cause a denial of service (uninitialized memory usage and system crash). Within Xen, 64-bit x86 PV Linux guest OS users can trigger a guest OS crash or possibly gain privileges.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4375
2294	CVE-2018-14665	HIGH	MEDIUM	A flaw was found in xorg-x11-server before 1.20.3. An incorrect permission check for -modulepath and -logfile options when starting Xorg. X server allows unprivileged users with the ability to log in to the system via physical console to escalate their privileges and run arbitrary code under root privileges.	xserver-xorg	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4916
2295	CVE-2018-14662	LOW	MEDIUM	The Ceph documentation states that clients should use "allow r" mon caps[1][2][3], which will grant full read access to all config-keys stored in the monitor -- including the LUKS encryption keys for OSD.	ceph	Unchanged	8.0.0.30	9.0.0.20	Won't Fix	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3398
2296	CVE-2018-14661	MEDIUM	MEDIUM	It was found that usage of snprintf function in feature/locks translator of glusterfs server 3.8.4, as shipped with Red Hat Gluster Storage, was vulnerable to a format string attack. A remote, authenticated attacker could use this flaw to cause remote denial of service.	glusterfs	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-5019
2297	CVE-2018-14660	MEDIUM	MEDIUM	A flaw was found in glusterfs server through versions 4.1.4 and 3.1.2 which allowed repeated usage of GF_META_LOCK_KEY xattr. A remote, authenticated attacker could use this flaw to create multiple locks for single inode by using setxattr repetitively resulting in memory exhaustion of glusterfs server node.	glusterfs	Unchanged	Not vulnerable	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-4982
2298	CVE-2018-14659	MEDIUM	MEDIUM	The Gluster file system through versions 4.1.4 and 3.1.2 is vulnerable to a denial of service attack via use of the 'GF_XATTR_IOSTATS_DUMP_KEY' xattr. A remote, authenticated attacker could exploit this by mounting a Gluster volume and repeatedly calling 'setxattr(2)' to trigger a state dump and create an arbitrary number of files in the server's runtime directory.	glusterfs	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-5029
2299	CVE-2018-14656	LOW	MEDIUM	A missing address check in the callers of the show_opcodes() in the Linux kernel allows an attacker to dump the kernel memory at an arbitrary kernel address into the dmesg log.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4784
2300	CVE-2018-14654	HIGH	MEDIUM	The Gluster file system through version 4.1.4 is vulnerable to abuse of the 'features/index' translator. A remote attacker with access to mount volumes could exploit this via the 'GF_XATTROP_ENTRY_IN_KEY' xattrop to create arbitrary, empty files on the target server.	glusterfs	Unchanged	Not vulnerable	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-5028
2301	CVE-2018-14653	MEDIUM	HIGH	The Gluster file system through versions 4.1.4 and 3.12 is vulnerable to a heap-based buffer overflow in the '__server_getspec' function via the 'gf_getspec_req' RPC message. A remote authenticated attacker could exploit this to cause a denial of service or other potential unspecified impact.	glusterfs	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-5027
2302	CVE-2018-14651	MEDIUM	HIGH	It was found that the fix for CVE-2018-10927, CVE-2018-10928, CVE-2018-10929, CVE-2018-10930, and CVE-2018-10926 was incomplete. A remote, authenticated attacker could use one of these flaws to execute arbitrary code, create arbitrary files, or cause denial of service on glusterfs server nodes via symlinks to relative paths.	glusterfs	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.4	Not vulnerable	Not vulnerable	LIN10-5001
2303	CVE-2018-14647	MEDIUM	HIGH	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make it easy to conduct denial of service attacks against Expat by constructing an XML document that would cause pathological hash collisions in Expat's internal data structures, consuming large amounts CPU and RAM. Python 3.8, 3.7, 3.6, 3.5, 3.4, 2.7 are believed to be vulnerable.	python	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	10.18.44.9	Not vulnerable	Vulnerable	LIN10-4821
2304	CVE-2018-14646	MEDIUM	MEDIUM	The Linux kernel before 4.15-rc8 was found to be vulnerable to a NULL pointer dereference bug in the __netlink_ns_capable() function in the net/netlink/af_netlink.c file. A local attacker could exploit this when a net namespace with a netnsid is assigned to cause a kernel panic and a denial of service.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-5071
2305	CVE-2018-14641	HIGH	MEDIUM	A security flaw was found in the ip_frag_reasm() function in net/ipv4/ip_fragment.c in the Linux kernel from 4.19-rc1 to 4.19-rc3 inclusive, which can cause a later system crash in ip_do_fragment(). With certain non-default, but non-rare, configuration of a victim host, an attacker can trigger this crash remotely, thus leading to a remote denial-of-service.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4811
2306	CVE-2018-14634	HIGH	HIGH	An integer overflow flaw was found in the Linux kernel's create_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.	linux	Unchanged	8.0.0.29	9.0.0.20	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4824

	A	B	C	D	E	F	G	H	I	J	K	L	M
2307	CVE-2018-14633	HIGH	HIGH	A security flaw was found in the chap_server_compute_md5() function in the ISCSI target code in the Linux kernel in a way an authentication request from an ISCSI initiator is processed. An unauthenticated remote attacker can cause a stack buffer overflow and smash up to 17 bytes of the stack. The attack requires the iSCSI target to be enabled on the victim host. Depending on how the target's code was built (i.e. depending on a compiler, compile flags and hardware architecture) an attack may lead to a system crash and thus to a denial-of-service or possibly to a non-authorized access to data exported by an iSCSI target. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although we believe it is highly unlikely. Kernel versions 4.18.x, 4.14.x and 3.10.x are believed to be vulnerable.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4775
2308	CVE-2018-14629	MEDIUM	MEDIUM	A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.	samba	Unchanged	Vulnerable	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3276
2309	CVE-2018-14627	MEDIUM	MEDIUM	The IIOP OpenJDK Subsystem in WildFly before version 14.0.0 does not honour configuration when SSL transport is required. Servers before this version that are configured with the following setting allow clients to create plaintext connections: <transport-config confidentiality=required trust-in-target=supported/>	wildfly	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9830
2310	CVE-2018-14625	MEDIUM	HIGH	A flaw was found in the Linux Kernel where an attacker may be able to have an uncontrolled read to kernel-memory from within a vm guest. A race condition between connect() and close() function may allow an attacker using the AF_VSOCK protocol to gather a 4 byte information leak or possibly intercept or corrupt AF_VSOCK messages destined to other clients.	linux	Unchanged	Not vulnerable	9.0.0.22	10.17.41.18	10.18.44.9	Not vulnerable	Not vulnerable	LIN10-4677
2311	CVE-2018-14622	MEDIUM	HIGH	A flaw was found in libtirpc. The return value of makefd_xprt was used without checking for NULL in svc_vc.c, leading to a null pointer dereference / segfault if the maximum number of available file descriptors was exhausted.	libtirpc	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4622
2312	CVE-2018-14621	HIGH	HIGH	A flaw was found in libtirpc before version 1.0.2-rc2. With the port to poll, and endless loop can be created when running out of file descriptors.	libtirpc	Unchanged	Not vulnerable	9.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4617
2313	CVE-2018-14619	HIGH	HIGH	A flaw was found in the crypto subsystem of the Linux kernel. The "null skcipher" was being by dropped in the wrong place -- when each af_alg_ctx was freed instead of when the aead_tfm was freed. This can cause the null skcipher to be freed while it is still in use. This may grant a local user to be able to crash the machine and possible corrupt memory leading to privilege escalation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4613
2314	CVE-2018-14618	HIGH	CRITICAL	curl before version 7.61.1 is vulnerable to a buffer overrun in the NTLM authentication code. The internal function Curl_ntlm_core_mk_nt_hash multiplies the length of the password by two (SUM) to figure out how large temporary storage area to allocate from the heap. The length value is then subsequently used to iterate over the password and generate output into the allocated storage buffer. On systems with a 32 bit size_t, the math to calculate SUM triggers an integer overflow when the password length exceeds 2GB (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the intended very huge one, making the use of that buffer end up in a heap buffer overflow. (This bug is almost identical to CVE-2017-8816.)	curl	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4713
2315	CVE-2018-14617	HIGH	MEDIUM	An issue was discovered in the Linux kernel through 4.17.10. There is a NULL pointer dereference and panic in hfsplus_lookup() in fs/hfsplus/dir.c when opening a file (that is purportedly a hard link) in an hfs+ filesystem that has malformed catalog data, and is mounted read-only without a metadata directory.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4437
2316	CVE-2018-14616	HIGH	MEDIUM	An issue was discovered in the Linux kernel through 4.17.10. There is a NULL pointer dereference in fscrypt_do_page_crypto() in fs/crypto/crypto.c when operating on a file in a corrupted f2fs image.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4447
2317	CVE-2018-14615	HIGH	MEDIUM	An issue was discovered in the Linux kernel through 4.17.10. There is a buffer overflow in truncate_inline_inode() in fs/f2fs/inline.c when umounting an f2fs image, because a length value may be negative.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4444
2318	CVE-2018-14614	HIGH	MEDIUM	An issue was discovered in the Linux kernel through 4.17.10. There is an out-of-bounds access in __remove_dirty_segment() in fs/f2fs/segment.c when mounting an f2fs image.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4434
2319	CVE-2018-14613	HIGH	MEDIUM	An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in io_ctl_map_page() when mounting and operating a crafted btrfs image, because of a lack of block group item validation in check_leaf_item in fs/btrfs/tree-checker.c.	linux	Unchanged	8.0.0.31	Vulnerable	10.17.41.19	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4442
2320	CVE-2018-14612	HIGH	MEDIUM	An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in btrfs_root_node() when mounting a crafted btrfs image, because of a lack of chunk block group mapping validation in btrfs_read_block_groups in fs/btrfs/extent-tree.c, and a lack of empty-tree checks in check_leaf in fs/btrfs/tree-checker.c.	linux	Unchanged	Not vulnerable	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4443
2321	CVE-2018-14611	HIGH	MEDIUM	An issue was discovered in the Linux kernel through 4.17.10. There is a use-after-free in try_merge_free_space() when mounting a crafted btrfs image, because of a lack of chunk type flag checks in btrfs_check_chunk_valid in fs/btrfs/volumes.c.	linux	Unchanged	8.0.0.29	9.0.0.20	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4421

	A	B	C	D	E	F	G	H	I	J	K	L	M
2322	CVE-2018-14610	HIGH	MEDIUM	An issue was discovered in the Linux kernel through 4.17.10. There is out-of-bounds access in write_extent_buffer() when mounting and operating a crafted btrfs image, because of a lack of verification that each block group has a corresponding chunk at mount time, within btrfs_read_block_groups in fs/btrfs/extent-tree.c.	linux	Unchanged	Not vulnerable	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4384
2323	CVE-2018-14609	HIGH	MEDIUM	An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in __del_reloc_root() in fs/btrfs/relocation.c when mounting a crafted btrfs image, related to removing reloc rb_trees when reloc control has not been initialized.	linux	Unchanged	8.0.0.29	9.0.0.20	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4446
2324	CVE-2018-14600	HIGH	CRITICAL	An issue was discovered in libX11 through 1.6.5. The function XListExtensions in ListExt.c interprets a variable as signed instead of unsigned, resulting in an out-of-bounds write (of up to 128 bytes), leading to DoS or remote code execution.	libx11	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4641
2325	CVE-2018-14599	HIGH	CRITICAL	An issue was discovered in libX11 through 1.6.5. The function XListExtensions in ListExt.c is vulnerable to an off-by-one error caused by malicious server responses, leading to DoS or possibly unspecified other impact.	libx11	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4629
2326	CVE-2018-14598	MEDIUM	HIGH	An issue was discovered in XListExtensions in ListExt.c in libX11 through 1.6.5. A malicious server can send a reply in which the first string overflows, causing a variable to be set to NULL that will be freed later on, leading to DoS (segmentation fault).	libx11	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4631
2327	CVE-2018-14567	MEDIUM	MEDIUM	Found a denial of service parsing a specially crafted xml file in libxml2 if liblzma-dev package is enabled.	libxml2	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-4486
2328	CVE-2018-14553	MEDIUM	HIGH	gdImageClone in gd.c in libgd 2.1.0-rc2 through 2.2.5 has a NULL pointer dereference allowing attackers to crash an application via a specific function call sequence. Only affects PHP when linked with an external libgd (not bundled).	gd	Updated	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.5	Not vulnerable	LIN1019-4035
2329	CVE-2018-14551	HIGH	CRITICAL	The ReadMATImageV4 function in coders/mat.c in ImageMagick 7.0.8-7 uses an uninitialized variable, leading to memory corruption.	imagemagick	Unchanged	8.0.0.27	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4419
2330	CVE-2018-14550	MEDIUM	HIGH	Stack-based buffer overflow in contrib/pngminus/pnm2png.c:get_token() function in libpng was found, possibly leading to arbitrary code execution when processing untrusted input.	libpng	Unchanged	8.0.0.31	Investigate	10.17.41.17	10.18.44.8	Not vulnerable	Not vulnerable	LIN1018-4176
2331	CVE-2018-14526	LOW	MEDIUM	An issue was discovered in rsn_supp/wpa.c in wpa_supplicant 2.0 through 2.6. Under certain conditions, the integrity of EAPOL-Key messages is not checked, leading to a decryption oracle. An attacker within range of the Access Point and client can abuse the vulnerability to recover sensitive information.	wpa-supplicant	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4532
2332	CVE-2018-14498	Medium	MEDIUM	get_8bit_row in rdbmp.c in libjpeg-turbo through 1.5.90 and MozJPEG through 3.3.1 allows attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted 8-bit BMP in which one or more of the color indices is out of range for the number of palette entries.	libjpeg-turbo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3785
2333	CVE-2018-14470	High	CRITICAL	The Babel parser in tcpdump before 4.9.3 has a buffer over-read in print-babel.c:babel_print_v2().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4991
2334	CVE-2018-14469	High	CRITICAL	The IKEv1 parser in tcpdump before 4.9.3 has a buffer over-read in print-isakmp.c:ikev1_n_print().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4990
2335	CVE-2018-14468	High	CRITICAL	The FRF.16 parser in tcpdump before 4.9.3 has a buffer over-read in print-fr.c:mfr_print().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4989
2336	CVE-2018-14467	High	CRITICAL	The BGP parser in tcpdump before 4.9.3 has a buffer over-read in print-bgp.c:bgp_capabilities_print() (BGP_CAPCODE_MP).	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4988
2337	CVE-2018-14466	High	CRITICAL	The Rx parser in tcpdump before 4.9.3 has a buffer over-read in print-rx.c:rx_cache_find() and rx_cache_insert().	tcpdump	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4987
2338	CVE-2018-14465	High	CRITICAL	The RSVP parser in tcpdump before 4.9.3 has a buffer over-read in print-rsvp.c:rsvp_obj_print().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4986
2339	CVE-2018-14464	High	CRITICAL	The LMP parser in tcpdump before 4.9.3 has a buffer over-read in print-lmp.c:lmp_print_data_link_subobjs().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4985
2340	CVE-2018-14463	High	CRITICAL	The VRRP parser in tcpdump before 4.9.3 has a buffer over-read in print-vrrp.c:vrrp_print().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4984
2341	CVE-2018-14462	High	CRITICAL	The ICMP parser in tcpdump before 4.9.3 has a buffer over-read in print-icmp.c:icmp_print().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4983
2342	CVE-2018-14461	High	CRITICAL	The LDP parser in tcpdump before 4.9.3 has a buffer over-read in print-ldp.c:ldp_tlv_print().	tcpdump	Unchanged	8.0.0.31	9.0.0.24	10.17.41.19	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4982
2343	CVE-2018-14438	MEDIUM	HIGH	In Wireshark through 2.6.2, the create_app_running_mutex function in wsutil/file_util.c calls SetSecurityDescriptorDacl to set a NULL DACL, which allows attackers to modify the access control arbitrarily.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4409
2344	CVE-2018-14437	MEDIUM	MEDIUM	ImageMagick 7.0.8-4 has a memory leak in parse8BIM in coders/meta.c.	imagemagick	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4393
2345	CVE-2018-14436	MEDIUM	MEDIUM	ImageMagick 7.0.8-4 has a memory leak in ReadMIFFImage in coders/miff.c.	imagemagick	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4462
2346	CVE-2018-14435	MEDIUM	MEDIUM	ImageMagick 7.0.8-4 has a memory leak in DecodeImage in coders/pcd.c.	imagemagick	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4448
2347	CVE-2018-14434	MEDIUM	MEDIUM	ImageMagick 7.0.8-4 has a memory leak for a colormap in WriteMPCImage in coders/mpc.c.	imagemagick	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4431
2348	CVE-2018-14424	MEDIUM	HIGH	The daemon in GDM through 3.29.1 does not properly unexport display objects from its D-Bus interface when they are destroyed, which allows a local attacker to trigger a use-after-free via a specially crafted sequence of D-Bus method calls, resulting in a denial of service or potential code execution.	gdm	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-7322
2349	CVE-2018-14423	MEDIUM	HIGH	Division-by-zero vulnerabilities in the functions pi_next_pcrl, pi_next_cprl, and pi_next_rpcl in lib/openjp3d/pi.c in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4645

	A	B	C	D	E	F	G	H	I	J	K	L	M
2350	CVE-2018-14404	MEDIUM	HIGH	A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 through 2.9.8 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case. Applications processing untrusted XSL format inputs with the use of the libxml2 library may be vulnerable to a denial of service attack due to a crash of the application.	libxml2	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4439
2351	CVE-2018-14395	MEDIUM	MEDIUM	libavformat/movenc.c in FFmpeg before 4.0.2 allows attackers to cause a denial of service (application crash caused by a divide-by-zero error) with a user crafted audio file when converting to the MOV audio format.	ffmpeg	Unchanged	Won't Fix	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4423
2352	CVE-2018-14394	MEDIUM	MEDIUM	libavformat/movenc.c in FFmpeg before 4.0.2 allows attackers to cause a denial of service (application crash caused by a divide-by-zero error) with a user crafted Waveform audio file.	ffmpeg	Unchanged	Won't Fix	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4390
2353	CVE-2018-14378			An issue was discovered in LibTIFF 4.0.9. A buffer overflow can occur via an invalid or empty tif argument to TIFFWriteBufferSetup in tif_write.c, and it can be exploited (at a minimum) via the following high-level library API function: TIFFWriteTile.	tiff	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4396
2354	CVE-2018-14375			An issue was discovered in LibTIFF 4.0.9. A buffer overflow vulnerability can occur via an invalid or empty tif argument to TIFFRGBAImageOK in tif_getimage.c, and it can be exploited (at a minimum) via the following high-level library API functions: TIFFReadRGBAImage, TIFFRGBAImageOK, and TIFFRGBAImageBegin.	tiff	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4412
2355	CVE-2018-14374			An issue was discovered in LibTIFF 4.0.9. A buffer overflow can occur via an empty fmt argument to unixErrorHandler in tif_unix.c, and it can be exploited (at a minimum) via the following high-level library API functions: TIFFClientOpen, TIFFFdOpen, TIFFRawStripSize, TIFFCheckTile, TIFFComputeStrip, TIFFReadRawTile, TIFFUnRegisterCODEC, and TIFFWriteEncodedTile.	tiff	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4370
2356	CVE-2018-14373			An issue was discovered in LibTIFF 4.0.9. In TIFFFindField in tif_dirinfo.c, the structure tif is being dereferenced without first checking that the structure is not empty and has the requested fields (tif_foundfield). In the call sequences following from the affected library functions (TIFFVGetField, TIFFVGetFieldDefaulted, TIFFVStripSize, TIFFScanlineSize, TIFFTileSize, TIFFGetFieldDefaulted, and TIFFGetField), this sanitization of the tif structure is never being done and, hence, using them with an invalid or empty tif structure will trigger a buffer overflow, leading to a crash.	tiff	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4449
2357	CVE-2018-14370	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.1 and 2.4.0 to 2.4.7, the IEEE 802.11 protocol dissector could crash. This was addressed in epan/crypt/airpdcap.c via bounds checking that prevents a buffer over-read.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4428
2358	CVE-2018-14369	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the HTTP2 dissector could crash. This was addressed in epan/dissectors/packet-http2.c by verifying that header data was found before proceeding to header decompression.	wireshark	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4435
2359	CVE-2018-14368	HIGH	HIGH	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the Bazaar protocol dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-bzr.c by properly handling items that are too long.	wireshark	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4432
2360	CVE-2018-14367	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.1 and 2.4.0 to 2.4.7, the CoAP protocol dissector could crash. This was addressed in epan/dissectors/packet-coap.c by properly checking for a NULL condition.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4380
2361	CVE-2018-14362	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. pop.c does not forbid characters that may have unsafe interaction with message-cache pathnames, as demonstrated by a '/' character.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9612
2362	CVE-2018-14359	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. They have a buffer overflow via base64 data.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9581
2363	CVE-2018-14358	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/message.c has a stack-based buffer overflow for a FETCH response with a long RFC822.SIZE field.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9531
2364	CVE-2018-14357	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. They allow remote IMAP servers to execute arbitrary commands via backquote characters, related to the mailboxes command associated with an automatic subscription.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9497
2365	CVE-2018-14356	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. pop.c mishandles a zero-length UID.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9538
2366	CVE-2018-14355	MEDIUM	MEDIUM	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/util.c mishandles .. directory traversal in a mailbox name.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9519
2367	CVE-2018-14354	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. They allow remote IMAP servers to execute arbitrary commands via backquote characters, related to the mailboxes command associated with a manual subscription or unsubscription.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9514
2368	CVE-2018-14353	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap_quote_string in imap/util.c has an integer underflow.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9537
2369	CVE-2018-14352	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap_quote_string in imap/util.c does not leave room for quote characters, leading to a stack-based buffer overflow.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9595
2370	CVE-2018-14351	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/command.c mishandles a long IMAP status mailbox literal count size.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9565

	A	B	C	D	E	F	G	H	I	J	K	L	M
2371	CVE-2018-14350	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/message.c has a stack-based buffer overflow for a FETCH response with a long INTERNALDATE field.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9602
2372	CVE-2018-14349	HIGH	CRITICAL	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/command.c mishandles a NO response without a message.	mutt	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9521
2373	CVE-2018-14348	MEDIUM	HIGH	libcgroup up to and including 0.41 creates /var/log/cgred with mode 0666 regardless of the configured umask, leading to disclosure of information.	libcgroup	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-4547
2374	CVE-2018-14344	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the ISMP dissector could crash. This was addressed in epan/dissectors/packet-ismp.c by validating the IPX address length to avoid a buffer over-read.	wireshark	Unchanged	Investigate	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4456
2375	CVE-2018-14343	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the ASN.1 BER dissector crash. This was addressed in epan/dissectors/packet-ber.c by ensuring that length values do not exceed the maximum signed integer.	wireshark	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4425
2376	CVE-2018-14342	HIGH	HIGH	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the BGP protocol dissector could go into a large loop. This was addressed in epan/dissectors/packet-bgp.c by validating Path Attribute lengths.	wireshark	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4464
2377	CVE-2018-14341	HIGH	HIGH	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the DICOM dissector could go into a large or infinite loop. This was addressed in epan/dissectors/packet-dcm.c by preventing an offset overflow.	wireshark	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4461
2378	CVE-2018-14340	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, dissectors that support zlib decompression could crash. This was addressed in epan/tvbuff_zlib.c by rejecting negative lengths to avoid a buffer over-read.	wireshark	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4413
2379	CVE-2018-14339	MEDIUM	HIGH	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the MMSE dissector could go into an infinite loop. This was addressed in epan/proto.c by adding offset and length validation.	wireshark	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4378
2380	CVE-2018-14056	MEDIUM	HIGH	ZNC before 1.7.1-rc1 is prone to a path traversal flaw via ../ in a web skin name to access files outside of the intended skins directories.	znc	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4330
2381	CVE-2018-14055	MEDIUM	MEDIUM	ZNC before 1.7.1-rc1 does not properly validate untrusted lines coming from the network, allowing a non-admin user to escalate his privilege and inject rogue values into znc.conf.	znc	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4296
2382	CVE-2018-14048	MEDIUM	MEDIUM	An issue has been found in libpng 1.6.34. It is a SEGV in the function png_free_data in png.c, related to the recommended error handling for png_read_image.	libpng	Unchanged	Vulnerable	Vulnerable	Vulnerable	Investigate	Not vulnerable	Not vulnerable	LIN10-4292
2383	CVE-2018-13988	MEDIUM	MEDIUM	Poppler through 0.62 contains a Buffer Overflow vulnerability due to an incorrect memory access that is not mapped in its memory space, as demonstrated by pdfunite. This can result in memory corruption and denial of service. This may be exploitable when a victim opens a specially crafted PDF file.	poppler	Unchanged	Won't Fix	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4383
2384	CVE-2018-13785	MEDIUM	MEDIUM	In libpng 1.6.34, a wrong calculation of row_factor in the png_check_chunk_length function (pngrutil.c) may trigger an integer overflow and resultant divide-by-zero while processing a crafted PNG file, leading to a denial of service.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4308
2385	CVE-2018-13458	MEDIUM	MEDIUM	qh_core in Nagios Core 4.4.1 and earlier is prone to a NULL pointer dereference vulnerability, which allows attackers to cause a local denial-of-service condition by sending a crafted payload to the listening UNIX socket.	nagios-core	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4313
2386	CVE-2018-13457	MEDIUM	MEDIUM	qh_echo in Nagios Core 4.4.1 and earlier is prone to a NULL pointer dereference vulnerability, which allows attackers to cause a local denial-of-service condition by sending a crafted payload to the listening UNIX socket.	nagios-core	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4286
2387	CVE-2018-13441	LOW	MEDIUM	qh_help in Nagios Core version 4.4.1 and earlier is prone to a NULL pointer dereference vulnerability, which allows attacker to cause a local denial-of-service condition by sending a crafted payload to the listening UNIX socket.	nagios-core	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4318
2388	CVE-2018-13440	MEDIUM	MEDIUM	The audiofile Audio File Library 0.3.6 has a NULL pointer dereference bug in ModuleState::setup in modules/ModuleState.cpp, which allows an attacker to cause a denial of service via a crafted caf file, as demonstrated by sfconvert.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4327
2389	CVE-2018-13420	MEDIUM	HIGH	** DISPUTED ** Google gperftools 2.7 has a memory leak in malloc_extension.cc, related to MallocExtension::Register and InitModule. NOTE: the software maintainer indicates that this is not a bug; it is only a false-positive report from the LeakSanitizer program.	gperftools	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Investigate	LIN1019-3673
2390	CVE-2018-13419	MEDIUM	HIGH	An issue has been found in libsndfile 1.0.28. There is a memory leak in psf_allocate in common.c, as demonstrated by sndfile-convert.	libsndfile1	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4323
2391	CVE-2018-13406	HIGH	HIGH	An integer overflow in the uvesafb_setcmap function in drivers/video/fbdev/uvesafb.c in the Linux kernel before 4.17.4 could result in local attackers being able to crash the kernel or potentially elevate privileges because kmalloc_array is not used.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4291
2392	CVE-2018-13405	MEDIUM	HIGH	The inode_init_owner function in fs/inode.c in the Linux kernel through 4.17.4 allows local users to create files with an unintended group ownership, in a scenario where a directory is SGID to a certain group and is writable by a user who is not a member of that group. Here, the non-member can trigger creation of a plain file whose group ownership is that group. The intended behavior was that the non-member can trigger creation of a directory (but not a plain file) whose group ownership is that group.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4274
2393	CVE-2018-13348	MEDIUM	HIGH	The mpatch_decode function in mpatch.c in Mercurial before 4.6.1 mishandles certain situations where there should be at least 12 bytes remaining after the current position in the patch data, but actually are not, aka OVE-20180430-0001.	mercurial	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4319
2394	CVE-2018-13347	HIGH	CRITICAL	mpatch.c in Mercurial before 4.6.1 mishandles integer addition and subtraction, aka OVE-20180430-0002.	mercurial	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4317

	A	B	C	D	E	F	G	H	I	J	K	L	M
2395	CVE-2018-13346	MEDIUM	HIGH	The mpatch_apply function in mpatch.c in Mercurial before 4.6.1 incorrectly proceeds in cases where the fragment start is past the end of the original data, aka OVE-20180430-0004.	mercurial	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4307
2396	CVE-2018-1333	MEDIUM	HIGH	By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).	apache	Unchanged	Not vulnerable	Vulnerable	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4389
2397	CVE-2018-13305	MEDIUM	HIGH	In FFmpeg 4.0.1, due to a missing check for negative values of the mquant variable, the vc1_put_blocks_clamped function in libavcodec/vc1_block.c may trigger an out-of-array access while converting a crafted AVI file to MPEG4, leading to an information disclosure or a denial of service.	ffmpeg	Unchanged	Won't Fix	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4293
2398	CVE-2018-13304	MEDIUM	MEDIUM	In libavcodec in FFmpeg 4.0.1, improper maintenance of the consistency between the context profile field and studio_profile in libavcodec may trigger an assertion failure while converting a crafted AVI file to MPEG4, leading to a denial of service, related to error_resilience.c, h263dec.c, and mpeg4videodec.c.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4324
2399	CVE-2018-13303	MEDIUM	MEDIUM	In FFmpeg 4.0.1, a missing check for failure of a call to init_get_bits8() in the avpriv_ac3_parse_header function in libavcodec/ac3_parser.c may trigger a NULL pointer dereference while converting a crafted AVI file to MPEG4, leading to a denial of service.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4279
2400	CVE-2018-13302	MEDIUM	HIGH	In FFmpeg 4.0.1, improper handling of frame types (other than EAC3_FRAME_TYPE_INDEPENDENT) that have multiple independent substreams in the handle_eac3 function in libavformat/movenc.c may trigger an out-of-array access while converting a crafted AVI file to MPEG4, leading to a denial of service or possibly unspecified other impact.	ffmpeg	Unchanged	Won't Fix	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4321
2401	CVE-2018-13301	MEDIUM	MEDIUM	In FFmpeg 4.0.1, due to a missing check of a profile value before setting it, the ff_mpeg4_decode_picture_header function in libavcodec/mpeg4videodec.c may trigger a NULL pointer dereference while converting a crafted AVI file to MPEG4, leading to a denial of service.	ffmpeg	Unchanged	Won't Fix	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4300
2402	CVE-2018-13300	MEDIUM	HIGH	In FFmpeg 4.0.1, an improper argument (AVCodecParameters) passed to the avpriv_request_sample function in the handle_eac3 function in libavformat/movenc.c may trigger an out-of-array read while converting a crafted AVI file to MPEG4, leading to a denial of service and possibly an information disclosure.	ffmpeg	Unchanged	Won't Fix	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4329
2403	CVE-2018-13259	HIGH	CRITICAL	An issue was discovered in zsh before 5.6. Shebang lines exceeding 64 characters were truncated, potentially leading to an execve call to a program name that is a substring of the intended one.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4705
2404	CVE-2018-1320	MEDIUM	HIGH	Apache Thrift Java client library versions 0.5.0 through 0.11.0 can bypass SASL negotiation isComplete validation in the org.apache.thrift.transport.TSaslTransport class. An assert used to determine if the SASL handshake had successfully completed could be disabled in production settings making the validation incomplete.	thrift	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3391
2405	CVE-2018-13153	MEDIUM	MEDIUM	In ImageMagick 7.0.8-4, there is a memory leak in the XMagickCommand function in MagickCore/animate.c.	imagemagick	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4297
2406	CVE-2018-13139	MEDIUM	HIGH	A stack-based buffer overflow in psf_memset in common.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted audio file. The vulnerability can be triggered by the executable sndfile-deinterleave.	libsndfile1	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-4326
2407	CVE-2018-1312	MEDIUM	CRITICAL	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.	apache	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3671
2408	CVE-2018-13112	MEDIUM	HIGH	get_l2len in common/get.c in Tcpreplay 4.3.0 beta 1 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via crafted packets, as demonstrated by tcpprep.	tcpreplay	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4294
2409	CVE-2018-13100	MEDIUM	MEDIUM	An issue was discovered in fs/f2fs/super.c in the Linux kernel through 4.17.3, which does not properly validate secs_per_zone in a corrupted f2fs image, as demonstrated by a divide-by-zero error.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4282
2410	CVE-2018-13099	MEDIUM	MEDIUM	An issue was discovered in fs/f2fs/inline.c in the Linux kernel through 4.17.3. A denial of service (out-of-bounds memory access and BUG) can occur for a modified f2fs filesystem image in which an inline inode contains an invalid reserved blkaddr.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4328
2411	CVE-2018-13098	MEDIUM	MEDIUM	An issue was discovered in fs/f2fs/inode.c in the Linux kernel through 4.17.3. A denial of service (slab out-of-bounds read and BUG) can occur for a modified f2fs filesystem image in which FI_EXTRA_ATTR is set in an inode.	linux	Unchanged	Not vulnerable	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4320
2412	CVE-2018-13097	MEDIUM	MEDIUM	An issue was discovered in fs/f2fs/super.c in the Linux kernel through 4.17.3. There is an out-of-bounds read or a divide-by-zero error for an incorrect user_block_count in a corrupted f2fs image, leading to a denial of service (BUG).	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4302
2413	CVE-2018-13096	MEDIUM	MEDIUM	An issue was discovered in fs/f2fs/super.c in the Linux kernel through 4.17.3. A denial of service (out-of-bounds memory access and BUG) can occur upon encountering an abnormal bitmap size when mounting a crafted f2fs image.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4301

	A	B	C	D	E	F	G	H	I	J	K	L	M
2414	CVE-2018-13095	MEDIUM	MEDIUM	An issue was discovered in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.17.3. A denial of service (memory corruption and BUG) can occur for a corrupted xfs image upon encountering an inode that is in extent format, but has more extents than fit in the inode fork.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4316
2415	CVE-2018-13094	MEDIUM	MEDIUM	An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occur for a corrupted xfs image after xfs_da_shrink_inode() is called with a NULL bp.	linux	Unchanged	Vulnerable	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4305
2416	CVE-2018-13093	MEDIUM	MEDIUM	An issue was discovered in fs/xfs/xfs_icache.c in the Linux kernel through 4.17.3. There is a NULL pointer dereference and panic in lookup_slow() on a NULL inode->i_ops pointer when doing pathwalks on a corrupted xfs image. This occurs because of a lack of proper validation that cached inodes are free during allocation.	linux	Unchanged	Vulnerable	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4284
2417	CVE-2018-13053	MEDIUM	HIGH	The alarm_timer_nsleep function in kernel/time/alarmtimer.c in the Linux kernel through 4.17.3 has an integer overflow via a large relative timeout because ktime_add_safe is not used.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4331
2418	CVE-2018-13033	MEDIUM	MEDIUM	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted ELF file, as demonstrated by _bfd_elf_parse_attributes in elf-attrs.c and bfd_malloc in libbfd.c. This can occur during execution of nm.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4283
2419	CVE-2018-1303	MEDIUM	HIGH	A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.	apache	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3651
2420	CVE-2018-1302	MEDIUM	MEDIUM	When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.	apache	Unchanged	Not vulnerable	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3659
2421	CVE-2018-1301	MEDIUM	MEDIUM	A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.	apache2	Unchanged	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3682
2422	CVE-2018-12934	MEDIUM	HIGH	remember_Ktype in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30, allows attackers to trigger excessive memory consumption (aka OOM). This can occur during execution of cxxfilt.	binutils	Unchanged	Vulnerable	Vulnerable	Vulnerable	Investigate	Not vulnerable	Not vulnerable	LIN10-4173
2423	CVE-2018-12931	HIGH	HIGH	ntfs_attr_find in the ntfs.ko filesystem driver in the Linux kernel 4.15.0 allows attackers to trigger a stack-based out-of-bounds write and cause a denial of service (kernel oops or panic) or possibly have unspecified other impact via a crafted ntfs filesystem.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4215
2424	CVE-2018-12930	HIGH	HIGH	ntfs_end_buffer_async_read in the ntfs.ko filesystem driver in the Linux kernel 4.15.0 allows attackers to trigger a stack-based out-of-bounds write and cause a denial of service (kernel oops or panic) or possibly have unspecified other impact via a crafted ntfs filesystem.	linux	Unchanged	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4218
2425	CVE-2018-12929	MEDIUM	MEDIUM	ntfs_read_locked_inode in the ntfs.ko filesystem driver in the Linux kernel 4.15.0 allows attackers to trigger a use-after-free read and possibly cause a denial of service (kernel oops or panic) via a crafted ntfs filesystem.	linux	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4179
2426	CVE-2018-12928	MEDIUM	MEDIUM	In the Linux kernel 4.15.0, a NULL pointer dereference was discovered in hfs_ext_read_extent in hfs.ko. This can occur during a mount of a crafted hfs filesystem.	linux	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4229
2427	CVE-2018-12911	HIGH	CRITICAL	WebKitGTK+ 2.20.3 has an off-by-one error, with a resultant out-of-bounds write, in the get_simple_globs functions in ThirdParty/xdgmime/src/xdgmimecache.c and ThirdParty/xdgmime/src/xdgmimeglob.c.	webkitgtk	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4381
2428	CVE-2018-12910	HIGH	CRITICAL	soup_cookie_jar_get_cookies in soup-cookie-jar.c in libsoup allows attackers to have unspecified impact via an empty hostname.	libsoup	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4289
2429	CVE-2018-12904	MEDIUM	MEDIUM	In arch/x86/kvm/vmx.c in the Linux kernel before 4.17.2, when nested virtualization is used, local attackers could cause L1 KVM guests to VMEXIT, potentially allowing privilege escalations and denial of service attacks due to lack of checking of CPL.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4189
2430	CVE-2018-12900	MEDIUM	HIGH	Heap-based buffer overflow in the cpSeparateBufToContigBuf function in tiffcp.c in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact via a crafted TIFF file.	tiff	Unchanged	Vulnerable	9.0.0.21	10.17.41.15	10.18.44.6	10.19.45.1	Not vulnerable	LIN10-4193
2431	CVE-2018-12896	LOW	MEDIUM	An issue was discovered in the Linux kernel through 4.17.3. An Integer Overflow in kernel/time/posix-timers.c in the POSIX timer code is caused by the way the overrun accounting works. Depending on interval and expiry time values, the overrun can be larger than INT_MAX, but the accounting is int based. This basically makes the accounting values, which are visible to user space via timer_getoverrun(2) and siginfo::si_overrun, random. For example, a local user can cause a denial of service (signed integer overflow) via crafted mmap, futex, timer_create, and timer_settime system calls.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4325

	A	B	C	D	E	F	G	H	I	J	K	L	M
2432	CVE-2018-12893	LOW	MEDIUM	An issue was discovered in Xen through 4.10.x. One of the fixes in XSA-260 added some safety checks to help prevent Xen livelocking with debug exceptions. Unfortunately, due to an oversight, at least one of these safety checks can be triggered by a guest. A malicious PV guest can crash Xen, leading to a Denial of Service. All Xen systems which have applied the XSA-260 fix are vulnerable. Only x86 systems are vulnerable. ARM systems are not vulnerable. Only x86 PV guests can exploit the vulnerability. x86 HVM and PVH guests cannot exploit the vulnerability. An attacker needs to be able to control hardware debugging facilities to exploit the vulnerability, but such permissions are typically available to unprivileged users.	xen	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4280
2433	CVE-2018-12892	MEDIUM	CRITICAL	An issue was discovered in Xen 4.7 through 4.10.x. libxl fails to pass the readonly flag to qemu when setting up a SCSI disk, due to what was probably an erroneous merge conflict resolution. Malicious guest administrators or (in some situations) users may be able to write to supposedly read-only disk images. Only emulated SCSI disks (specified as sd in the libxl disk configuration, or an equivalent) are affected. IDE disks (hd) are not affected (because attempts to make them readonly are rejected). Additionally, CDROM devices (that is, devices specified to be presented to the guest as CDROMs, regardless of the nature of the backing storage on the host) are not affected; they are always read only. Only systems using qemu-xen (rather than qemu-xen-traditional) as the device model version are vulnerable. Only systems using libxl or libxl-based toolstacks are vulnerable. (This includes xl, and libvirt with the libxl driver.) The vulnerability is present in Xen versions 4.7 and later. (In earlier versions, provided that the patch for XSA-142 has been applied, attempts to create read only disks are rejected.) If the host and guest together usually support PVHVM, the issue is exploitable only if the malicious guest administrator has control of the guest kernel or guest kernel command line.	xen	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4309
2434	CVE-2018-12891	MEDIUM	MEDIUM	An issue was discovered in Xen through 4.10.x. Certain PV MMU operations may take a long time to process. For that reason Xen explicitly checks for the need to preempt the current vCPU at certain points. A few rarely taken code paths did bypass such checks. By suitably enforcing the conditions through its own page table contents, a malicious guest may cause such bypasses to be used for an unbounded number of iterations. A malicious or buggy PV guest may cause a Denial of Service (DoS) affecting the entire host. Specifically, it may prevent use of a physical CPU for an indeterminate period of time. All Xen versions from 3.4 onwards are vulnerable. Xen versions 3.3 and earlier are vulnerable to an even wider class of attacks, due to them lacking preemption checks altogether in the affected code paths. Only x86 systems are affected. ARM systems are not affected. Only multi-vCPU x86 PV guests can leverage the vulnerability. x86 HVM or PVH guests as well as x86 single-vCPU PV ones cannot leverage the vulnerability.	xen	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4314
2435	CVE-2018-12886	Medium	HIGH	stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack canary is compared against.	gcc	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4138
2436	CVE-2018-12882	HIGH	CRITICAL	exif_read_from_impl in ext/exif/exif.c in PHP 7.2.x through 7.2.7 allows attackers to trigger a use-after-free (in exif_read_from_file) because it closes a stream that it is not responsible for closing. The vulnerable code is reachable through the PHP exif_read_data function.	php	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4204
2437	CVE-2018-1283	LOW	MEDIUM	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a Session header. This comes from the HTTP_SESSION variable name used by mod_session to forward its data to CGIs, since the prefix HTTP_ is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.	apache	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3662
2438	CVE-2018-12714	HIGH	CRITICAL	An issue was discovered in the Linux kernel through 4.17.2. The filter parsing in kernel/trace/trace_events_filter.c could be called with no filter, which is an N=0 case when it expected at least one line to have been read, thus making the N-1 index invalid. This allows attackers to cause a denial of service (slab out-of-bounds write) or possibly have unspecified other impact via crafted perf_event_open and mmap system calls.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4198
2439	CVE-2018-12713	MEDIUM	CRITICAL	GIMP through 2.10.2 makes g_get_tmp_dir calls to establish temporary filenames, which may result in a filename that already exists, as demonstrated by the gimp_write_and_read_file function in app/tests/test-xcf.c. This might be leveraged by attackers to overwrite files or read file content that was intended to be private.	gimp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4195
2440	CVE-2018-12700	MEDIUM	HIGH	A Stack Exhaustion issue was discovered in debug_write_type in debug.c in GNU Binutils 2.30 because of DEBUG_KIND_INDIRECT infinite recursion.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4197

	A	B	C	D	E	F	G	H	I	J	K	L	M
2441	CVE-2018-12699	HIGH	CRITICAL	finish_stab in stabs.c in GNU Binutils 2.30 allows attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact, as demonstrated by an out-of-bounds write of 8 bytes. This can occur during execution of objdump.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4210
2442	CVE-2018-12698	MEDIUM	HIGH	demangle_template in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30, allows attackers to trigger excessive memory consumption (aka OOM) during the Create an array for saving the template argument values XNEWVEC call. This can occur during execution of objdump.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4234
2443	CVE-2018-12697	MEDIUM	HIGH	A NULL pointer dereference (aka SEGV on unknown address 0x000000000000) was discovered in work_stuff_copy_to_from in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. This can occur during execution of objdump.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4200
2444	CVE-2018-12641	MEDIUM	MEDIUM	An issue was discovered in arm_pt in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_arm_hp_template, demangle_class_name, demangle_fund_type, do_type, do_arg, demangle_args, and demangle_nested_args. This can occur during execution of nm-new.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-4175
2445	CVE-2018-12633	MEDIUM	MEDIUM	An issue was discovered in the Linux kernel through 4.17.2. vbg_misc_device_ioctl() in drivers/virt/vboxguest/vboxguest_linux.c reads the same user data twice with copy_from_user. The header part of the user data is double-fetched, and a malicious user thread can tamper with the critical variables (hdr.size_in and hdr.size_out) in the header between the two fetches because of a race condition, leading to severe kernel errors, such as buffer over-accesses. This bug can cause a local denial of service and information leakage.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4183
2446	CVE-2018-12617	MEDIUM	HIGH	qmp_guest_file_read in qga/commands-posix.c and qga/commands-win32.c in qemu-ga (aka QEMU Guest Agent) in QEMU 2.12.50 has an integer overflow causing a g_malloc0() call to trigger a segmentation fault when trying to allocate a large memory chunk. The vulnerability can be exploited by sending a crafted QMP command (including guest-file-read with a large count value) to the agent via the listening socket.	qemu	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4227
2447	CVE-2018-12613	MEDIUM	HIGH	An issue was discovered in phpMyAdmin 4.8.x before 4.8.2, in which an attacker can include (view and potentially execute) files on the server. The vulnerability comes from a portion of code where pages are redirected and loaded within phpMyAdmin, and an improper test for whitelisted pages. An attacker must be authenticated, except in the $cfg['AllowArbitraryServer'] = true case (where an attacker can specify any host he/she is already in control of, and execute arbitrary code on phpMyAdmin) and the $cfg['ServerDefault'] = 0 case (which bypasses the login requirement and runs the vulnerable code without any authentication).	phpmyadmin	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4228
2448	CVE-2018-12600	MEDIUM	HIGH	In ImageMagick 7.0.8-3 Q16, ReadDIBImage and WriteDIBImage in coders/dib.c allow attackers to cause an out of bounds write via a crafted file.	imagemagick	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4221
2449	CVE-2018-12599	MEDIUM	HIGH	In ImageMagick 7.0.8-3 Q16, ReadBMPImage and WriteBMPImage in coders/bmp.c allow attackers to cause an out of bounds write via a crafted file.	imagemagick	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4211
2450	CVE-2018-12581	MEDIUM	MEDIUM	An issue was discovered in js/designer/move.js in phpMyAdmin before 4.8.2. A Cross-Site Scripting vulnerability has been found where an attacker can use a crafted database name to trigger an XSS attack when that database is referenced from the Designer feature.	phpmyadmin	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4233
2451	CVE-2018-12551	Medium	HIGH	When Eclipse Mosquitto version 1.0 to 1.5.5 (inclusive) is configured to use a password file for authentication, any malformed data in the password file will be treated as valid. This typically means that the malformed data becomes a username and no password. If this occurs, clients can circumvent authentication and get access to the broker by using the malformed username. In particular, a blank line will be treated as a valid empty username. Other security measures are unaffected. Users who have only used the mosquitto_passwd utility to create and modify their password files are unaffected by this vulnerability.	mosquitto	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3812
2452	CVE-2018-12550	Medium	HIGH	When Eclipse Mosquitto version 1.0 to 1.5.5 (inclusive) is configured to use an ACL file, and that ACL file is empty, or contains only comments or blank lines, then Mosquitto will treat this as though no ACL file has been defined and use a default allow policy. The new behaviour is to have an empty ACL file mean that all access is denied, which is not a useful configuration but is not unexpected.	mosquitto	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3814
2453	CVE-2018-12546	Medium	MEDIUM	In Eclipse Mosquitto version 1.0 to 1.5.5 (inclusive) when a client publishes a retained message to a topic, then has its access to that topic revoked, the retained message will still be published to clients that subscribe to that topic in the future. In some applications this may result in clients being able cause effects that would otherwise not be allowed.	mosquitto	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3815
2454	CVE-2018-12543	MEDIUM	HIGH	In Eclipse Mosquitto versions 1.5 to 1.5.2 inclusive, if a message is published to Mosquitto that has a topic starting with $, but that is not $SYS, e.g. $test/test, then an assert is triggered that should otherwise not be reachable and Mosquitto will exit.	mosquitto	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-5010

	A	B	C	D	E	F	G	H	I	J	K	L	M
2455	CVE-2018-12460	MEDIUM	MEDIUM	libavcodec in FFmpeg 4.0 may trigger a NULL pointer dereference if the studio profile is incorrectly detected while converting a crafted AVI file to MPEG4, leading to a denial of service, related to idctdsp.c and mpegvideo.c.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4169
2456	CVE-2018-12459	MEDIUM	MEDIUM	An inconsistent bits-per-sample value in the ff_mpeg4_decode_picture_header function in libavcodec/mpeg4videodec.c in FFmpeg 4.0 may trigger an assertion violation while converting a crafted AVI file to MPEG4, leading to a denial of service.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4166
2457	CVE-2018-12458	MEDIUM	MEDIUM	An improper integer type in the mpeg4_encode_gop_header function in libavcodec/mpeg4videoenc.c in FFmpeg 4.0 may trigger an assertion violation while converting a crafted AVI file to MPEG4, leading to a denial of service.	ffmpeg	Unchanged	Won't Fix	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4191
2458	CVE-2018-12453	MEDIUM	HIGH	Type confusion in the xgroupCommand function in t_stream.c in redis-server in Redis before 5.0 allows remote attackers to cause denial-of-service via an XGROUP command in which the key is not a stream.	redis	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4170
2459	CVE-2018-12436	LOW	MEDIUM	wolfcrypt/src/ecc.c in wolfSSL before 3.15.1.patch allows a memory-cache side-channel attack on ECDSA signatures, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.	wolfssl	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Won't Fix	Won't Fix	Won't Fix	LIN10-4116
2460	CVE-2018-12422	HIGH	CRITICAL	** DISPUTED ** addressbook/backends/ldap/e-book-backend-ldap.c in Evolution-Data-Server in GNOME Evolution through 3.29.2 might allow attackers to trigger a Buffer Overflow via a long query that is processed by the strcat function. NOTE: the software maintainer disputes this because the code had computed the required string length first, and then allocated a large-enough buffer on the heap.	evolution-data-server	Updated	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Won't Fix	LIN1019-3674
2461	CVE-2018-12404	MEDIUM	MEDIUM	An issue was found in nss before version 3.36.6. The TLS implementation exposes padding oracle in each of the three stages of handling PKCS #1 v1.5 padding	nss	Unchanged	Vulnerable	Vulnerable	Vulnerable	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3333
2462	CVE-2018-12384	MEDIUM	MEDIUM	A flaw was found with NSS library when compiled with a server application. A man-in-the-middle attacker could use this flaw in a passive replay attack.	nss	Unchanged	Investigate	Investigate	Investigate	10.18.44.3	Not vulnerable	Not vulnerable	LIN10-5069
2463	CVE-2018-12327	HIGH	CRITICAL	Stack-based buffer overflow in ntpq and ntpdc of NTP version 4.2.8p11 allows an attacker to achieve code execution or escalate to higher privileges via a long string as the argument for an IPv4 or IPv6 command-line parameter. NOTE: It is unclear whether there are any common situations in which ntpq or ntpdc is used with a command line from an untrusted source.	ntp	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4181
2464	CVE-2018-12326	MEDIUM	HIGH	Buffer overflow in redis-cli of Redis before 4.0.10 and 5.x before 5.0 RC3 allows an attacker to achieve code execution and escalate to higher privileges via a crafted command line. NOTE: It is unclear whether there are any common situations in which redis-cli is used with, for example, a -h (aka hostname) argument from an untrusted source.	redis	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4167
2465	CVE-2018-12294	MEDIUM	HIGH	WebCore/platform/graphics/texmap/TextureMapperLayer.cpp in WebKit, as used in WebKitGTK+ prior to version 2.20.2, is vulnerable to a use after free for a WebCore::TextureMapperLayer object.	webkitgtk	Unchanged	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4188
2466	CVE-2018-12293	MEDIUM	HIGH	The getImageData function in the ImageBufferCairo class in WebCore/platform/graphics/cairo/ImageBufferCairo.cpp in WebKit, as used in WebKitGTK+ prior to version 2.20.3 and WPE WebKit prior to version 2.20.1, is vulnerable to a heap-based buffer overflow triggered by an integer overflow, which could be abused by crafted HTML content.	webkitgtk	Unchanged	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4222
2467	CVE-2018-12233	MEDIUM	HIGH	In the ea_get function in fs/jfs/xattr.c in the Linux kernel through 4.17.1, a memory corruption bug in JFS can be triggered by calling setxattr twice with two different extended attribute names on the same file. This vulnerability can be triggered by an unprivileged user with the ability to create files and execute programs. A kmalloc call is incorrect, leading to slab-out-of-bounds in jfs_xattr.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4123
2468	CVE-2018-12232	HIGH	MEDIUM	In net/socket.c in the Linux kernel through 4.17.1, there is a race condition between fchownat and close in cases where they target the same socket file descriptor, related to the sock_close and sockfs_setattr functions. fchownat does not increment the file descriptor reference count, which allows close to set the socket to NULL during fchownat's execution, leading to a NULL pointer dereference and system crash.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4113
2469	CVE-2018-12207	MEDIUM	MEDIUM	Improper invalidation for page table updates by a virtual guest operating system for multiple Intel(R) Processors may allow an authenticated user to potentially enable denial of service of the host system via local access.	linux	Unchanged	Investigate	Investigate	Investigate	Investigate	10.19.45.1	10.20.6.0	LIN1019-3669
2470	CVE-2018-12130	Medium	MEDIUM	Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.17	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-4077

	A	B	C	D	E	F	G	H	I	J	K	L	M
2471	CVE-2018-12127	Medium	MEDIUM	Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.17	10.18.44.7	Not vulnerable	Not vulnerable	LIN1018-4076
2472	CVE-2018-12126	Medium	MEDIUM	Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.17	Investigate	Not vulnerable	Not vulnerable	LIN1018-4075
2473	CVE-2018-12021	MEDIUM	MEDIUM	Singularity 2.3.0 through 2.5.1 is affected by an incorrect access control on systems supporting overlay file system. When using the overlay option, a malicious user may access sensitive information by exploiting a few specific Singularity features.	singularity	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4277
2474	CVE-2018-12020	MEDIUM	HIGH	mainproc.c in GnuPG before 2.2.8 mishandles the original filename during decryption and verification actions, which allows remote attackers to spoof the output that GnuPG sends on file descriptor 2 to other programs that use the --status-fd 2 option. For example, the OpenPGP data might represent an original filename that contains line feed characters in conjunction with GOODSIG or VALIDSIG status codes.	gnupg	Unchanged	8.0.0.27	9.0.0.17	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4114
2475	CVE-2018-12015	MEDIUM	HIGH	In Perl through 5.26.2, the Archive::Tar module allows remote attackers to bypass a directory-traversal protection mechanism, and overwrite arbitrary files, via an archive file containing a symlink and a regular file with the same name.	perl	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4115
2476	CVE-2018-11813	MEDIUM	HIGH	libjpeg 9c has a large loop because read_pixel in rdtarga.c mishandles EOF.	libjpeg-turbo	Unchanged	Won't Fix	9.0.0.21	10.17.41.15	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4576
2477	CVE-2018-11806	HIGH	HIGH	m_cat in slirp/mbuf.c in Qemu has a heap-based buffer overflow via incoming fragmented datagrams.	qemu	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4127
2478	CVE-2018-11803	Medium	HIGH	Subversion's mod_dav_svn Apache HTTPD module versions 1.11.0 and 1.10.0 to 1.10.3 will crash after dereferencing an uninitialized pointer if the client omits the root path in a recursive directory listing operation.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	10.18.44.4	Not vulnerable	Not vulnerable	LIN1018-3582
2479	CVE-2018-11798	MEDIUM	MEDIUM	The Apache Thrift Node.js static web server in versions 0.9.2 through 0.11.0 have been determined to contain a security vulnerability in which a remote user has the ability to access files outside the set webservers docroot path.	thrift	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3396
2480	CVE-2018-11782	Medium	MEDIUM	In Apache Subversion versions up to and including 1.9.10, 1.10.4, 1.12.0, Subversion's svnserve server process may exit when a well-formed read-only request produces a particular answer. This can lead to disruption for users of the server.	subversion	Unchanged	Investigate	9.0.0.24	10.17.41.19	10.18.44.12	Not vulnerable	Not vulnerable	LIN1018-5004
2481	CVE-2018-11763	MEDIUM	MEDIUM	In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.	apache	Unchanged	Not vulnerable	Investigate	10.17.41.13	Vulnerable	Not vulnerable	Vulnerable	LIN10-4789
2482	CVE-2018-11713	MEDIUM	MEDIUM	WebCore/platform/network/soup/SocketStreamHandleImplSoup.cpp in the libsoup network backend of WebKit, as used in WebKitGTK+ prior to version 2.20.0 or without libsoup 2.62.0, unexpectedly failed to use system proxy settings for WebSocket connections. As a result, users could be deanonymized by crafted web sites via a WebSocket connection.	webkitgtk	Unchanged	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4111
2483	CVE-2018-11712	MEDIUM	HIGH	WebCore/platform/network/soup/SocketStreamHandleImplSoup.cpp in the libsoup network backend of WebKit, as used in WebKitGTK+ versions 2.20.0 and 2.20.1, failed to perform TLS certificate verification for WebSocket connections.	webkitgtk	Unchanged	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4112
2484	CVE-2018-11656	MEDIUM	MEDIUM	In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function ReadDCMImage in coders/dcm.c, which allows attackers to cause a denial of service via a crafted DCM image file.	imagemagick	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4120
2485	CVE-2018-11655	MEDIUM	MEDIUM	In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function GetImagePixelCache in MagickCore/cache.c, which allows attackers to cause a denial of service via a crafted CALS image file.	imagemagick	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4119
2486	CVE-2018-11652	HIGH	CRITICAL	CSV Injection vulnerability in Nikto 2.1.6 and earlier allows remote attackers to inject arbitrary OS commands via the Server field in an HTTP response header, which is directly injected into a CSV report.	nikto	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4100
2487	CVE-2018-11645	MEDIUM	MEDIUM	psi/zfile.c in Artifex Ghostscript before 9.21rc1 permits the status command even if -dSAFER is used, which might allow remote attackers to determine the existence and size of arbitrary files, a similar issue to CVE-2016-7977.	ghostscript	Unchanged	8.0.0.27	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4105
2488	CVE-2018-11625	Medium	HIGH	In ImageMagick 7.0.7-37 Q16, SetGrayscaleImage in the quantize.c file allows attackers to cause a heap-based buffer over-read via a crafted file.	imagemagick	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4124
2489	CVE-2018-11624	Medium	HIGH	In ImageMagick 7.0.7-36 Q16, the ReadMATImage function in coders/mat.c allows attackers to cause a use after free via a crafted file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4108
2490	CVE-2018-11529	MEDIUM	HIGH	VideoLAN VLC media player 2.2.x is prone to a use after free vulnerability which an attacker can leverage to execute arbitrary code via crafted MKV files. Failed exploit attempts will likely result in denial of service conditions.	vlc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4332
2491	CVE-2018-1152	MEDIUM	MEDIUM	libjpeg-turbo 1.5.90 is vulnerable to a denial of service vulnerability caused by a divide by zero when processing a crafted BMP image.	libjpeg-turbo	Unchanged	Won't Fix	9.0.0.18	10.17.41.11	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4217
2492	CVE-2018-11508	LOW	MEDIUM	The compat_get_timex function in kernel/compat.c in the Linux kernel before 4.16.9 allows local users to obtain sensitive information from kernel memory via adjtimex.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4026

	A	B	C	D	E	F	G	H	I	J	K	L	M
2493	CVE-2018-11506	HIGH	HIGH	The sr_do_ioctl function in drivers/scsi/sr_ioctl.c in the Linux kernel through 4.16.12 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact because sense buffers have different sizes at the CDROM layer and the SCSI layer.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4031
2494	CVE-2018-11490	MEDIUM	HIGH	The DGifDecompressLine function in dgif_lib.c in GIFLIB (possibly version 3.0.x), as later shipped in cgif.c in sam2p 0.49.4, has a heap-based buffer overflow because a certain Private->RunningCode - 2 array index is not checked. This will lead to a denial of service or possibly unspecified other impact.	giflib	Unchanged	Won't Fix	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4045
2495	CVE-2018-11489	MEDIUM	HIGH	The DGifDecompressLine function in dgif_lib.c in GIFLIB (possibly version 3.0.x), as later shipped in cgif.c in sam2p 0.49.4, has a heap-based buffer overflow because a certain CrntCode array index is not checked. This will lead to a denial of service or possibly unspecified other impact.	giflib	Unchanged	Won't Fix	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4041
2496	CVE-2018-11439	MEDIUM	MEDIUM	The TagLib::Ogg::FLAC::File::scan function in oggflacfile.cpp in TagLib 1.11.1 allows remote attackers to cause information disclosure (heap-based buffer over-read) via a crafted audio file.	taglib	Unchanged	8.0.0.30	9.0.0.21	10.17.41.13	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-4044
2497	CVE-2018-11412	MEDIUM	MEDIUM	In the Linux kernel 4.13 through 4.16.11, ext4_read_inline_data() in fs/ext4/inline.c performs a memcpy with an untrusted length value in certain circumstances involving a crafted filesystem that stores the system.data extended attribute value in a dedicated inode.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4058
2498	CVE-2018-1140	LOW	MEDIUM	A missing input sanitization flaw was found in the implementation of LDP database used for the LDAP server. An attacker could use this flaw to cause a denial of service against a samba server, used as a Active Directory Domain Controller. All versions of Samba from 4.8.0 onwards are vulnerable	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4619
2499	CVE-2018-11396	MEDIUM	HIGH	ephy-session.c in libephymain.so in GNOME Web (aka Epiphany) through 3.28.2.1 allows remote attackers to cause a denial of service (application crash) via JavaScript code that triggers access to a NULL URL, as demonstrated by a crafted window.open call.	epiphany	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4038
2500	CVE-2018-1139	MEDIUM	HIGH	A flaw was found in the way samba before 4.7.9 and 4.8.4 allowed the use of weak NTLMv1 authentication even when NTLMv1 was explicitly disabled. A man-in-the-middle attacker could use this flaw to read the credential and other details passed between the samba server and client.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4639
2501	CVE-2018-11362	MEDIUM	HIGH	In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the LDSS dissector could crash. This was addressed in epan/dissectors/packet-ldss.c by avoiding a buffer over-read upon encountering a missing '\0' character.	wireshark	Unchanged	Not vulnerable	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4063
2502	CVE-2018-11361	MEDIUM	HIGH	In Wireshark 2.6.0, the IEEE 802.11 protocol dissector could crash. This was addressed in epan/crypt/dot11decrypt.c by avoiding a buffer overflow during FTE processing in Dot11DecryptTDLSDeriveKey.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4059
2503	CVE-2018-11360	MEDIUM	HIGH	In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the GSM A DTAP dissector could crash. This was addressed in epan/dissectors/packet-gsm_a_dtap.c by fixing an off-by-one error that caused a buffer overflow.	wireshark	Unchanged	Not vulnerable	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4052
2504	CVE-2018-11359	MEDIUM	HIGH	In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the RRC dissector and other dissectors could crash. This was addressed in epan/proto.c by avoiding a NULL pointer dereference.	wireshark	Unchanged	Not vulnerable	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4028
2505	CVE-2018-11358	MEDIUM	HIGH	In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the Q.931 dissector could crash. This was addressed in epan/dissectors/packet-q931.c by avoiding a use-after-free after a malformed packet prevented certain cleanup.	wireshark	Unchanged	Not vulnerable	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4027
2506	CVE-2018-11357	MEDIUM	HIGH	In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the LTP dissector and other dissectors could consume excessive memory. This was addressed in epan/tvbuff.c by rejecting negative lengths.	wireshark	Unchanged	Not vulnerable	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4037
2507	CVE-2018-11356	MEDIUM	HIGH	In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the DNS dissector could crash. This was addressed in epan/dissectors/packet-dns.c by avoiding a NULL pointer dereference for an empty name in an SRV record.	wireshark	Unchanged	Not vulnerable	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4060
2508	CVE-2018-11355	MEDIUM	HIGH	In Wireshark 2.6.0, the RTCP dissector could crash. This was addressed in epan/dissectors/packet-rtcp.c by avoiding a buffer overflow for packet status chunks.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4054
2509	CVE-2018-11354	MEDIUM	HIGH	In Wireshark 2.6.0, the IEEE 1905.1a dissector could crash. This was addressed in epan/dissectors/packet-ieee1905.c by making a certain correction to string handling.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4040
2510	CVE-2018-1130	MEDIUM	MEDIUM	Linux kernel before version 4.16-rc7 is vulnerable to a null pointer dereference in dccp_write_xmit() function in net/dccp/output.c in that allows a local user to cause a denial of service by a number of certain crafted system calls.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3940
2511	CVE-2018-1129	LOW	MEDIUM	A flaw was found in the way signature calculation was handled by cephx authentication protocol. An attacker having access to ceph cluster network who is able to alter the message payload was able to bypass signature checks done by cephx protocol. Ceph branches master, mimic, luminous and jewel are believed to be vulnerable.	ceph	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4276
2512	CVE-2018-1128	MEDIUM	HIGH	It was found that cephx authentication protocol did not verify ceph clients correctly and was vulnerable to replay attack. Any attacker having access to ceph cluster network who is able to sniff packets on network can use this vulnerability to authenticate with ceph service and perform actions allowed by ceph service. Ceph branches master, mimic, luminous and jewel are believed to be vulnerable.	ceph	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4311
2513	CVE-2018-1126	HIGH	CRITICAL	procps-ng before version 3.3.15 is vulnerable to an incorrect integer size in proc/alloc.* leading to truncation/integer overflow issues. This flaw is related to CVE-2018-1124.	procps	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3985

	A	B	C	D	E	F	G	H	I	J	K	L	M
2514	CVE-2018-11251	MEDIUM	MEDIUM	In ImageMagick 7.0.7-23 Q16 x86_64 2018-01-24, there is a heap-based buffer over-read in ReadSUNImage in coders/sun.c, which allows attackers to cause a denial of service (application crash in SetGrayscaleImage in MagickCore/quantize.c) via a crafted SUN image file.	imagemagick	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4048
2515	CVE-2018-1125	MEDIUM	HIGH	procps-ng before version 3.3.15 is vulnerable to a stack buffer overflow in pgrep. This vulnerability is mitigated by FORTIFY, as it involves strncat() to a stack-allocated string. When pgrep is compiled with FORTIFY (as on Red Hat Enterprise Linux and Fedora), the impact is limited to a crash.	procps	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3984
2516	CVE-2018-1124	MEDIUM	HIGH	procps-ng before version 3.3.15 is vulnerable to multiple integer overflows leading to a heap corruption in file2strvec function. This allows a privilege escalation for a local attacker who can create entries in procfs by starting processes, which could result in crashes or arbitrary code execution in proc utilities run by other users.	procps	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3983
2517	CVE-2018-11237	MEDIUM	HIGH	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.27 and earlier may write data beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.	glibc	Unchanged	Not vulnerable	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4035
2518	CVE-2018-11236	MEDIUM	HIGH	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution.	glibc	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4050
2519	CVE-2018-11235	MEDIUM	HIGH	In Git before 2.13.7, 2.14.x before 2.14.4, 2.15.x before 2.15.2, 2.16.x before 2.16.4, and 2.17.x before 2.17.1, remote code execution can occur. With a crafted .gitmodules file, a malicious project can execute an arbitrary script on a machine that runs git clone --recurse-submodules because submodule names are obtained from this file, and then appended to $GIT_DIR/modules, leading to directory traversal with ../ in a name. Finally, post-checkout hooks from a submodule are executed, bypassing the intended design in which hooks are not obtained from a remote server.	git	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4061
2520	CVE-2018-11233	MEDIUM	HIGH	In Git before 2.13.7, 2.14.x before 2.14.4, 2.15.x before 2.15.2, 2.16.x before 2.16.4, and 2.17.x before 2.17.1, code to sanity-check pathnames on NTFS can result in reading out-of-bounds memory.	git	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4053
2521	CVE-2018-11232	MEDIUM	MEDIUM	The etm_setup_aux function in drivers/hwtracing/coresight/coresight-etm-perf.c in the Linux kernel before 4.10.2 allows attackers to cause a denial of service (panic) because a parameter is incorrectly used as a local variable.	linux	Unchanged	Not vulnerable	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4049
2522	CVE-2018-1123	MEDIUM	HIGH	procps-ng before version 3.3.15 is vulnerable to a denial of service in ps via mmap buffer overflow. Inbuilt protection in ps maps a guard page at the end of the overflowed buffer, ensuring that the impact of this flaw is limited to a crash (temporary denial of service).	procps	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3982
2523	CVE-2018-11224	MEDIUM	MEDIUM	An issue was discovered in Libav 12.3. A read access violation in the in_table_init16 function in libavcodec/aacsbr.c allows remote attackers to cause a denial of service (application crash), as demonstrated by avconv.	libav	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4064
2524	CVE-2018-1122	MEDIUM	HIGH	procps-ng before version 3.3.15 is vulnerable to a local privilege escalation in top. If a user runs top with HOME unset in an attacker-controlled directory, the attacker could achieve privilege escalation by exploiting one of several vulnerabilities in the config_file() function.	procps	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3981
2525	CVE-2018-11219	HIGH	CRITICAL	An Integer Overflow issue was discovered in the struct library in the Lua subsystem in Redis before 3.2.12, 4.x before 4.0.10, and 5.x before 5.0 RC2, leading to a failure of bounds checking.	redis	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4171
2526	CVE-2018-11218	HIGH	CRITICAL	Memory Corruption was discovered in the cmsgpack library in the Lua subsystem in Redis before 3.2.12, 4.x before 4.0.10, and 5.x before 5.0 RC2 because of stack-based buffer overflows.	redis	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4225
2527	CVE-2018-1121	MEDIUM	MEDIUM	An unprivileged attacker can hide a process from procps-ng's utilities, by exploiting either a denial of service (a rather noisy method) or a race condition inherent in reading /proc/PID entries (a stealthier method).?	linux	Unchanged	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3980
2528	CVE-2018-1120	LOW	MEDIUM	An attacker can block any read() access to /proc/PID/cmdline by mmap()ing a FUSE file (Filesystem in Userspace) onto this process's command-line arguments. The attacker can therefore block pgrep, pidof, pkill, ps, and w, either forever (a denial of service), or for some controlled time (a synchronization tool for exploiting other Vulnerabilities)	linux	Unchanged	8.0.0.29	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3979
2529	CVE-2018-1118	LOW	MEDIUM	Linux kernel vhost since version 4.8 does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.	linux	Unchanged	Not vulnerable	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3929
2530	CVE-2018-1116	LOW	HIGH	A flaw was found in polkit before version 0.116. The implementation of the polkit_backend_interactive_authority_check_authorization function in polkitd allows to test for authentication and trigger authentication of unrelated processes owned by other users. This may result in a local DoS and information disclosure.	polkit	Unchanged	Won't Fix	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4290
2531	CVE-2018-1115	MEDIUM	CRITICAL	postgresql before versions 10.4, 9.6.9 is vulnerable in the adminpack extension, the pg_catalog.pg_logfile_rotate() function doesn't follow the same ACLs than pg_rorate_logfile. If the adminpack is added to a database, an attacker able to connect to it could exploit this to force log rotation.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3931

	A	B	C	D	E	F	G	H	I	J	K	L	M
2532	CVE-2018-1112	HIGH	HIGH	glusterfs server before versions 3.10.12, 4.0.2 is vulnerable when using 'auth.allow' option which allows any unauthenticated gluster client to connect from any network to mount gluster storage volumes. NOTE: this vulnerability exists because of a CVE-2018-1088 regression.	glusterfs	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3863
2533	CVE-2018-11102	MEDIUM	HIGH	An issue was discovered in Libav 12.3. A read access violation in the mov_probe function in libavformat/mov.c allows remote attackers to cause a denial of service (application crash), as demonstrated by avconv.	libav	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3925
2534	CVE-2018-1108	MEDIUM	MEDIUM	kernel drivers before version 4.17-rc1 are vulnerable to a weakness in the Linux kernel's implementation of random seed data. Programs, early in the boot sequence, could use the data allocated for the seed before it was sufficiently generated.	linux	Unchanged	Not vulnerable	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4032
2535	CVE-2018-1100	HIGH	HIGH	zsh through version 5.4.2 is vulnerable to a stack-based buffer overflow in the utils.c:checkmailpath function. A local attacker could exploit this to execute arbitrary code in the context of another user.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3754
2536	CVE-2018-10963	MEDIUM	MEDIUM	The TIFFWriteDirectorySec() function in tif_dirwrite.c in LibTIFF through 4.0.9 allows remote attackers to cause a denial of service (assertion failure and application crash) via a crafted file.	libtiff	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3941
2537	CVE-2018-1095	HIGH	MEDIUM	The ext4_xattr_check_entries function in fs/ext4/xattr.c in the Linux kernel through 4.15.15 does not properly validate xattr sizes, which causes misinterpretation of a size as an error code, and consequently allows attackers to cause a denial of service (get_acl NULL pointer dereference and system crash) via a crafted ext4 image.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3670
2538	CVE-2018-10940	MEDIUM	MEDIUM	The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows local attackers to use a incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3935
2539	CVE-2018-1094	HIGH	MEDIUM	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.15.15 does not always initialize the crc32c checksum driver, which allows attackers to cause a denial of service (ext4_xattr_inode_hash NULL pointer dereference and system crash) via a crafted ext4 image.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3661
2540	CVE-2018-10938	HIGH	MEDIUM	A flaw was found in the Linux kernel present since v4.0-rc1 and through v4.13-rc4. A crafted network packet sent remotely by an attacker may force the kernel to enter an infinite loop in the cipso_v4_optptr() function in net/ipv4/cipso_ipv4.c leading to a denial-of-service.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4628
2541	CVE-2018-10933	Medium	CRITICAL	A vulnerability was found in libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, resulting in unauthorized access.	libssh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4879
2542	CVE-2018-10930	MEDIUM	MEDIUM	A flaw was found in RPC request using gfs3_rename_req in glusterfs server. An authenticated attacker could use this flaw to write to a destination outside the gluster volume.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4712
2543	CVE-2018-1093	HIGH	MEDIUM	The ext4_valid_block_bitmap function in fs/ext4/balloc.c in the Linux kernel through 4.15.15 allows attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image because balloc.c and ialloc.c do not validate bitmap block numbers.	linux	Unchanged	8.0.0.27	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3644
2544	CVE-2018-10929	MEDIUM	HIGH	A flaw was found in RPC request using gfs2_create_req in glusterfs server. An authenticated attacker could use this flaw to create arbitrary files and execute arbitrary code on glusterfs server nodes.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4699
2545	CVE-2018-10928	MEDIUM	HIGH	A flaw was found in RPC request using gfs3_symlink_req in glusterfs server which allows symlink destinations to point to file paths outside of the gluster volume. An authenticated attacker could use this flaw to create arbitrary symlinks pointing anywhere on the server and execute arbitrary code on glusterfs server nodes.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4721
2546	CVE-2018-10927	MEDIUM	HIGH	A flaw was found in RPC request using gfs3_lookup_req in glusterfs server. An authenticated attacker could use this flaw to leak information and execute remote denial of service by crashing gluster brick process.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4697
2547	CVE-2018-10926	MEDIUM	HIGH	A flaw was found in RPC request using gfs3_mknod_req supported by glusterfs server. An authenticated attacker could use this flaw to write files to an arbitrary location via path traversal and execute arbitrary code on a glusterfs server node.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4736
2548	CVE-2018-10925	MEDIUM	HIGH	It was discovered that PostgreSQL versions before 10.5, 9.6.10, 9.5.14, 9.4.19, and 9.3.24 failed to properly check authorization on certain statements involved with INSERT ... ON CONFLICT DO UPDATE. An attacker with CREATE TABLE privileges could exploit this to read arbitrary bytes server memory. If the attacker also had certain INSERT and limited UPDATE privileges to a particular table, they could exploit this to update other columns in the same table.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4546
2549	CVE-2018-10924	MEDIUM	MEDIUM	It was discovered that fsync(2) system call in glusterfs client code leaks memory. An authenticated attacker could use this flaw to launch a denial of service attack by making gluster clients consume memory of the host machine.	glusterfs	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4709
2550	CVE-2018-10923	MEDIUM	HIGH	It was found that the mknod call derived from mknod(2) can create files pointing to devices on a glusterfs server node. An authenticated attacker could use this to create an arbitrary device and read data from any device attached to the glusterfs server node.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4689

	A	B	C	D	E	F	G	H	I	J	K	L	M
2551	CVE-2018-1092	HIGH	MEDIUM	The ext4_iget function in fs/ext4/inode.c in the Linux kernel through 4.15.15 mishandles the case of a root directory with a zero i_links_count, which allows attackers to cause a denial of service (ext4_process_freed_data NULL pointer dereference and OOPS) via a crafted ext4 image.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3634
2552	CVE-2018-10919	MEDIUM	MEDIUM	The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.	samba	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4586
2553	CVE-2018-10918	MEDIUM	MEDIUM	A null pointer dereference flaw was found in the way samba checked database outputs from the LDB database layer. An authenticated attacker could use this flaw to crash a samba server in an Active Directory Domain Controller configuration. Samba versions before 4.7.9 and 4.8.4 are vulnerable.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4612
2554	CVE-2018-10916	HIGH	MEDIUM	It has been discovered that lftp up to and including version 4.8.3 does not properly sanitize remote file names, leading to a loss of integrity on the local system when reverse mirroring is used. A remote attacker may trick a user to use reverse mirroring on an attacker controlled FTP server, resulting in the removal of all files in the current working directory of the victim's system.	lftp	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4537
2555	CVE-2018-10915	MEDIUM	HIGH	A vulnerability was found in libpq, the default PostgreSQL client library where libpq failed to properly reset its internal state between connections. If an affected version of libpq was used with host or hostaddr connection parameters from untrusted input, attackers could bypass client-side connection security features, obtain access to higher privileged connections or potentially cause other impact through SQL injection, by causing the PQescape() functions to malfunction. Postgresql versions before 10.5, 9.6.10, 9.5.14, 9.4.19, and 9.3.24 are affected.	postgresql	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4542
2556	CVE-2018-10914	MEDIUM	MEDIUM	It was found that an attacker could issue a xattr request via glusterfs FUSE to cause gluster brick process to crash which will result in a remote denial of service. If gluster multiplexing is enabled this will result in a crash of multiple bricks and gluster volumes.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4710
2557	CVE-2018-10913	MEDIUM	MEDIUM	An information disclosure vulnerability was discovered in glusterfs server. An attacker could issue a xattr request via glusterfs FUSE to determine the existence of any file.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4741
2558	CVE-2018-10911	MEDIUM	HIGH	A flaw was found in the way dic_unserialize function of glusterfs does not handle negative key length values. An attacker could use this flaw to read memory from other locations into the stored dict value.	glusterfs	Unchanged	8.0.0.28	Investigate	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4679
2559	CVE-2018-1091	MEDIUM	MEDIUM	In the flush_tmregs_to_thread function in arch/powerpc/kernel/ptrace.c in the Linux kernel before 4.13.5, a guest kernel crash can be triggered from unprivileged userspace during a core dump on a POWER host due to a missing processor feature check and an erroneous use of transactional memory (TM) instructions in the core dump path, leading to a denial of service.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3674
2560	CVE-2018-10907	MEDIUM	HIGH	It was found that glusterfs server is vulnerable to multiple stack based buffer overflows due to functions in server-rpc-fopc.c allocating fixed size buffers using 'alloca(3)'. An authenticated attacker could exploit this by mounting a gluster volume and sending a string longer that the fixed buffer size to cause crash or potential code execution.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4740
2561	CVE-2018-10906	MEDIUM	HIGH	In fuse before versions 2.9.8 and 3.x before 3.2.5, fusermount is vulnerable to a restriction bypass when SELinux is active. This allows non-root users to mount a FUSE file system with the 'allow_other' mount option regardless of whether 'user_allow_other' is set in the fuse configuration. An attacker may use this flaw to mount a FUSE file system, accessible by other users, and trick them into accessing files on that file system, possibly causing Denial of Service or other unspecified effects.	fuse	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4440
2562	CVE-2018-10904	MEDIUM	HIGH	It was found that glusterfs server does not properly sanitize file paths in the trusted.io-stats-dump extended attribute which is used by the debug/io-stats translator. Attacker can use this flaw to create files and execute arbitrary code. To exploit this attacker would require sufficient access to modify the extended attributes of files on a gluster volume.	glusterfs	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4698
2563	CVE-2018-10903	MEDIUM	HIGH	A flaw was found in python-cryptography versions between >=1.9.0 and <2.3. The finalize_with_tag API did not enforce a minimum tag length. If a user did not validate the input length prior to passing it to finalize_with_tag an attacker could craft an invalid payload with a shortened tag (e.g. 1 byte) such that they would have a 1 in 256 chance of passing the MAC check. GCM tag forgeries can cause key leakage.	python-cryptography	Unchanged	Not vulnerable	Not vulnerable	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4407
2564	CVE-2018-10902	MEDIUM	HIGH	It was found that the raw midi kernel driver does not protect against concurrent access which leads to a double realloc (double free) in snd_rawmidi_input_params() and snd_rawmidi_output_status() which are part of snd_rawmidi_ioctl() handler in rawmidi.c file. A malicious local attacker could possibly use this for privilege escalation.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4642
2565	CVE-2018-10901	HIGH	HIGH	A flaw was found in Linux kernel's KVM virtualization subsystem. The VMX code does not restore the GDT.LIMIT to the previous host value, but instead sets it to 64KB. With a corrupted GDT limit a host's userspace code has an ability to place malicious entries in the GDT, particularly to the per-cpu variables. An attacker can use this to escalate their privileges.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4405

	A	B	C	D	E	F	G	H	I	J	K	L	M
2566	CVE-2018-10896	LOW	HIGH	The default cloud-init configuration, in cloud-init 0.6.2 and newer, included ssh_deletekeys: 0, disabling cloud-init's deletion of ssh host keys. In some environments, this could lead to instances created by cloning a golden master or template system, sharing ssh host keys, and being able to impersonate one another or conduct man-in-the-middle attacks.	cloud-init	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4525
2567	CVE-2018-10888	MEDIUM	MEDIUM	A flaw was found in libgit2 before version 0.27.3. A missing check in git_delta_apply function in delta.c file, may lead to an out-of-bound read while reading a binary delta file. An attacker may use this flaw to cause a Denial of Service.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4303
2568	CVE-2018-10887	MEDIUM	HIGH	A flaw was found in libgit2 before version 0.27.3. It has been discovered that an unexpected sign extension in git_delta_apply function in delta.c file may lead to an integer overflow which in turn leads to an out of bound read, allowing to read before the base object. An attacker may use this flaw to leak memory addresses or cause a Denial of Service.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4304
2569	CVE-2018-10883	MEDIUM	MEDIUM	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write in jbd2_journal_dirty_metadata(), a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4387
2570	CVE-2018-10882	MEDIUM	MEDIUM	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound write in in fs/jbd2/transaction.c code, a denial of service, and a system crash by unmounting a crafted ext4 filesystem image.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4391
2571	CVE-2018-10881	MEDIUM	MEDIUM	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4373
2572	CVE-2018-10880	HIGH	MEDIUM	Linux kernel is vulnerable to a stack-out-of-bounds write in the ext4 filesystem code when mounting and writing to a crafted ext4 image in ext4_update_inline_data(). An attacker could use this to cause a system crash and a denial of service.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4397
2573	CVE-2018-1088	MEDIUM	HIGH	A privilege escalation flaw was found in gluster 3.x snapshot scheduler. Any gluster client allowed to mount gluster volumes could also mount shared gluster storage volume and escalate privileges by scheduling malicious cronjob via symlink.	glusterfs	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3930
2574	CVE-2018-10879	MEDIUM	HIGH	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause a use-after-free in ext4_xattr_set_entry function and a denial of service or unspecified other impact may occur by renaming a file in a crafted ext4 filesystem image.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4408
2575	CVE-2018-10878	MEDIUM	HIGH	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write and a denial of service or unspecified other impact is possible by mounting and operating a crafted ext4 filesystem image.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4377
2576	CVE-2018-10877	MEDIUM	MEDIUM	Linux kernel ext4 filesystem is vulnerable to an out-of-bound access in the ext4_ext_drop_refs() function when operating on a crafted ext4 filesystem image.	linux	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4372
2577	CVE-2018-10876	MEDIUM	MEDIUM	A flaw was found in Linux kernel in the ext4 filesystem code. A use-after-free is possible in ext4_ext_remove_space() function when mounting and operating a crafted ext4 image.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4429
2578	CVE-2018-10873	MEDIUM	HIGH	A vulnerability was discovered in SPICE before version 0.14.1 where the generated code used for demarshalling messages lacked sufficient bounds checks. A malicious client or server, after authentication, could send specially crafted messages to its peer which would result in a crash or, potentially, other impacts.	spice	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4607
2579	CVE-2018-1087	MEDIUM	HIGH	A flaw was found in the way the Linux kernel's KVM hypervisor handled exceptions delivered after a stack switch operation via Mov SS or Pop SS instructions. During the stack switch operation, processor does not deliver interrupts and exceptions, they are delivered once the first instruction after the stack switch is executed.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3887
2580	CVE-2018-10862	MEDIUM	MEDIUM	WildFly Core before version 6.0.0.Alpha3 does not properly validate file paths in .war archives, allowing for the extraction of crafted .war archives to overwrite arbitrary files. This is an instance of the 'Zip Slip' vulnerability.	wildfly	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9525
2581	CVE-2018-10861	MEDIUM	HIGH	A flaw was found in the way ceph mon handles user requests. Any authenticated ceph user having read access to ceph can delete, create ceph storage pools and corrupt snapshot images. Ceph branches master, mimic, luminous and jewel are believed to be affected.	ceph	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4310
2582	CVE-2018-10858	MEDIUM	HIGH	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.	samba	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4591
2583	CVE-2018-10853	MEDIUM	HIGH	A flaw was found in Linux Kernel KVM versions greater than and including 4.10. In which certain instructions such as sgdt/sidt call segmented_write_std doesn't propagate access correctly. As such, during userspace induced exception, the guest can incorrectly assume that the exception happened in the kernel and panic.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4190
2584	CVE-2018-10852	MEDIUM	HIGH	The UNIX pipe which sudo uses to contact SSSD and read the available sudo rules from SSSD has too wide permissions, which means that anyone who can send a message using the same raw protocol that sudo and SSSD use can read the sudo rules available for any user. This affects versions of SSSD before 1.16.3.	sssd	Unchanged	Not vulnerable	Won't Fix	Won't Fix	10.18.44.15	Won't Fix	Won't Fix	LIN10-4203

	A	B	C	D	E	F	G	H	I	J	K	L	M
2585	CVE-2018-10846	LOW	MEDIUM	A cache-based side channel in GnuTLS implementation that leads to plain text recovery in cross-VM attack setting was found. An attacker could use a combination of Just in Time Prime+probe attack in combination with Lucky-13 attack to recover plain text using crafted packets.	gnutls	Unchanged	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4595
2586	CVE-2018-10845	MEDIUM	MEDIUM	It was found that the GnuTLS implementation of HMAC-SHA-384 was vulnerable to a Lucky thirteen style attack. Remote attackers could use this flaw to conduct distinguishing attacks and plain text recovery attacks via statistical analysis of timing data using crafted packets.	gnutls	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4640
2587	CVE-2018-10844	MEDIUM	MEDIUM	It was found that the GnuTLS implementation of HMAC-SHA-256 was vulnerable to a Lucky thirteen style attack. Remote attackers could use this flaw to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data using crafted packets.	gnutls	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4643
2588	CVE-2018-10841	MEDIUM	HIGH	glusterfs is vulnerable to privilege escalation on gluster server nodes. An authenticated gluster client via TLS could use gluster cli with --remote-host command to add it self to trusted storage pool and perform privileged gluster operations like adding other machines to trusted storage pool, start, stop, and delete volumes.	glusterfs	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4177
2589	CVE-2018-10840	HIGH	MEDIUM	The Linux kernel is vulnerable to a heap-based buffer overflow in the fs/ext4/xattr.c:ext4_xattr_set_entry() function. An attacker could exploit this by operating on a mounted crafted ext4 image.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4231
2590	CVE-2018-1084	HIGH	CRITICAL	corosync before version 2.4.4 is vulnerable to an integer overflow in exec/totemcrypto.c.	corosync	Unchanged	8.0.0.26	Won't Fix	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3744
2591	CVE-2018-10839	MEDIUM	MEDIUM	Qemu emulator <= 3.0.0 built with the NE2000 NIC emulation support is vulnerable to an integer overflow, which could lead to buffer overflow issue. It could occur when receiving packets over the network. A user inside guest could use this flaw to crash the Qemu process resulting in DoS.	qemu	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4863
2592	CVE-2018-1083	HIGH	HIGH	Zsh before version 5.4.2-test-1 is vulnerable to a buffer overflow in the shell autocomplete functionality. A local unprivileged user can create a specially crafted directory path which leads to code execution in the context of the user who tries to use autocomplete to traverse the before mentioned path. If the user affected is privileged, this leads to privilege escalation.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3672
2593	CVE-2018-10811	MEDIUM	HIGH	strongSwan 5.6.0 and older allows Remote Denial of Service because of Missing Initialization of a Variable.	strongswan	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4185
2594	CVE-2018-10805	MEDIUM	MEDIUM	ImageMagick version 7.0.7-28 contains a memory leak in ReadYCBCRImage in coders/ycbcr.c.	imagemagick	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3923
2595	CVE-2018-10804	MEDIUM	MEDIUM	ImageMagick version 7.0.7-28 contains a memory leak in WriteTIFFImage in coders/tiff.c.	imagemagick	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3926
2596	CVE-2018-10801	MEDIUM	MEDIUM	TIFFClientOpen in tif_unix.c in LibTIFF 3.8.2 has memory leaks, as demonstrated by bmp2tiff.	libtiff	Unchanged	Vulnerable	Vulnerable	Vulnerable	Investigate	Not vulnerable	Not vulnerable	LIN10-3936
2597	CVE-2018-10779	MEDIUM	HIGH	TIFFWriteScanline in tif_write.c in LibTIFF 3.8.2 has a heap-based buffer over-read, as demonstrated by bmp2tiff.	libtiff	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3928
2598	CVE-2018-10768	MEDIUM	HIGH	There is a NULL pointer dereference in the AnnotPath::getCoordsLength function in Annot.h in an Ubuntu package for Poppler 0.24.5. A crafted input will lead to a remote denial of service attack. Later Ubuntu packages such as for Poppler 0.41.0 are not affected.	poppler	Unchanged	Won't Fix	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3933
2599	CVE-2018-10754	MEDIUM	HIGH	In ncurses before 6.1.20180414, there is a NULL Pointer Dereference in the _nc_parse_entry function of tinfo/parse_entry.c. It could lead to a remote denial of service if the terminfo library code is used to process untrusted terminfo data in which a use-name is invalid syntax.	ncurses	Unchanged	8.0.0.27	9.0.0.17	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3932
2600	CVE-2018-1071	LOW	MEDIUM	zsh through version 5.4.2 is vulnerable to a stack-based buffer overflow in the exec.c:hashcmd() function. A local attacker could exploit this to cause a denial of service.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3559
2601	CVE-2018-10689	MEDIUM	MEDIUM	blktrace (aka Block IO Tracing) 1.2.0, as used with the Linux kernel and Android, has a buffer overflow in the dev_map_read function in btt/devmap.c because the device and devno arrays are too small, as demonstrated by an invalid free when using the btt program with a crafted file.	blktrace	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-3922
2602	CVE-2018-1068	HIGH	MEDIUM	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3658
2603	CVE-2018-10675	HIGH	HIGH	The do_get_mempolicy function in mm/mempolicy.c in the Linux kernel before 4.12.9 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted system calls.	linux	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3905
2604	CVE-2018-1066	HIGH	MEDIUM	The Linux kernel before version 4.11 is vulnerable to a NULL pointer dereference in fs/cifs/cifsencrypt.c:setup_ntlmv2_rsp() that allows an attacker controlling a CIFS server to kernel panic a client that has this server mounted, because an empty Targetinfo field in an NTLMSSP setup negotiation response is mishandled during session recovery.	linux	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3540
2605	CVE-2018-1065	MEDIUM	MEDIUM	The netfilter subsystem in the Linux kernel through 4.15.7 mishandles the case of a rule blob that contains a jump but lacks a user-defined chain, which allows local users to cause a denial of service (NULL pointer dereference) by leveraging the CAP_NET_RAW or CAP_NET_ADMIN capability, related to arpt_do_table in net/ipv4/netfilter/arp_tables.c, ipt_do_table in net/ipv4/netfilter/ip_tables.c, and ip6t_do_table in net/ipv6/netfilter/ip6_tables.c.	linux	Unchanged	Not vulnerable	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3561

	A	B	C	D	E	F	G	H	I	J	K	L	M
2606	CVE-2018-1064	MEDIUM	HIGH	libvirt version before 4.2.0-rc1 is vulnerable to a resource exhaustion as a result of an incomplete fix for CVE-2018-5748 that affects QEMU monitor but now also triggered via QEMU guest agent.	libvirt	Unchanged	8.0.0.26	9.0.0.16	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3665
2607	CVE-2018-1063	LOW	MEDIUM	Context relabeling of filesystems is vulnerable to symbolic link attack, allowing a local, unprivileged malicious entity to change the SELinux context of an arbitrary file to a context with few restrictions. This only happens when the relabeling process is done, usually when taking SELinux state from disabled to enable (permissive or enforcing). The issue was found in policycoreutils 2.5-11.	policycoreutils	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3585
2608	CVE-2018-1061	MEDIUM	HIGH	python before versions 2.7.15, 3.4.9, 3.5.6 and 3.7.0 is vulnerable to catastrophic backtracking in the difflib.IS_LINE_JUNK method. An attacker could use this flaw to cause denial of service.	python	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4201
2609	CVE-2018-1060	MEDIUM	HIGH	python before versions 2.7.15, 3.4.9, 3.5.6 and 3.7.0 is vulnerable to catastrophic backtracking in pop3lib's apop() method. An attacker could use this flaw to cause denial of service.	python	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4192
2610	CVE-2018-1059	LOW	MEDIUM	The DPDK vhost-user interface does not check to verify that all the requested guest physical range is mapped and contiguous when performing Guest Physical Addresses to Host Virtual Addresses translations. This may lead to a malicious guest exposing vhost-user backend process memory. All versions before 18.02.1 are vulnerable.	dpdk	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3198
2611	CVE-2018-1058	MEDIUM	HIGH	A flaw was found in the way Postgresql allowed a user to modify the behavior of a query for other users. An attacker with a user account could use this flaw to execute code with the permissions of superuser in the database. Versions 9.3 through 10 are affected.	postgresql	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3563
2612	CVE-2018-1057	MEDIUM	HIGH	On a Samba 4 AD DC the LDAP server in all versions of Samba from 4.0.0 onwards incorrectly validates permissions to modify passwords over LDAP allowing authenticated users to change any other users' passwords, including administrative users and privileged service accounts (eg Domain Controllers).	samba	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3534
2613	CVE-2018-10549	MEDIUM	HIGH	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final \0' character.	php	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3860
2614	CVE-2018-10548	MEDIUM	HIGH	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.	php	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3857
2615	CVE-2018-10547	MEDIUM	MEDIUM	An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.	php	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3822
2616	CVE-2018-10546	MEDIUM	HIGH	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.	php	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3826
2617	CVE-2018-10545	LOW	MEDIUM	An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.	php	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3824
2618	CVE-2018-10540	MEDIUM	MEDIUM	An issue was discovered in WavPack 5.1.0 and earlier for W64 input. Out-of-bounds writes can occur because ParseWave64HeaderConfig in wave64.c does not validate the sizes of unknown chunks before attempting memory allocation, related to a lack of integer-overflow protection within a bytes_to_copy calculation and subsequent malloc call, leading to insufficient memory allocation.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3859
2619	CVE-2018-10539	MEDIUM	MEDIUM	An issue was discovered in WavPack 5.1.0 and earlier for DSDiff input. Out-of-bounds writes can occur because ParseDsdiffHeaderConfig in dsdiff.c does not validate the sizes of unknown chunks before attempting memory allocation, related to a lack of integer-overflow protection within a bytes_to_copy calculation and subsequent malloc call, leading to insufficient memory allocation.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3801
2620	CVE-2018-10538	MEDIUM	MEDIUM	An issue was discovered in WavPack 5.1.0 and earlier for WAV input. Out-of-bounds writes can occur because ParseRiffHeaderConfig in riff.c does not validate the sizes of unknown chunks before attempting memory allocation, related to a lack of integer-overflow protection within a bytes_to_copy calculation and subsequent malloc call, leading to insufficient memory allocation.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3867
2621	CVE-2018-10537	MEDIUM	HIGH	An issue was discovered in WavPack 5.1.0 and earlier. The W64 parser component contains a vulnerability that allows writing to memory because ParseWave64HeaderConfig in wave64.c does not reject multiple format chunks.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3800
2622	CVE-2018-10536	MEDIUM	HIGH	An issue was discovered in WavPack 5.1.0 and earlier. The WAV parser component contains a vulnerability that allows writing to memory because ParseRiffHeaderConfig in riff.c does not reject multiple format chunks.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3840

	A	B	C	D	E	F	G	H	I	J	K	L	M
2623	CVE-2018-10535	MEDIUM	MEDIUM	The ignore_section_sym function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, does not validate the output_section pointer in the case of a symtab entry with a SECTION type that has a 0 value, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file, as demonstrated by objcopy.	binutils	Unchanged	8.0.0.27	9.0.0.20	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3841
2624	CVE-2018-10534	MEDIUM	MEDIUM	The _bfd_XX_bfd_copy_private_bfd_data_common function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, processes a negative Data Directory size with an unbounded loop that increases the value of (external_IMAGE_DEBUG_DIRECTORY) *edd so that the address exceeds its own memory region, resulting in an out-of-bounds memory write, as demonstrated by objcopy copying private info with _bfd_pex64_bfd_copy_private_bfd_data_common in pex64igen.c.	binutils	Unchanged	8.0.0.27	9.0.0.20	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3810
2625	CVE-2018-1053	LOW	HIGH	In postgresql 9.3.x before 9.3.21, 9.4.x before 9.4.16, 9.5.x before 9.5.11, 9.6.x before 9.6.7 and 10.x before 10.2, pg_upgrade creates file in current working directory containing the output of `pg_dumpall -g` under umask which was in effect when the user invoked pg_upgrade, and not under 0077 which is normally used for other temporary files. This can allow an authenticated attacker to read or modify the one file, which may contain encrypted or unencrypted database passwords. The attack is infeasible if a directory mode blocks the attacker searching the current working directory or if the prevailing umask blocks the attacker opening the file.	postgresql	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3370
2626	CVE-2018-1052	MEDIUM	MEDIUM	Memory disclosure vulnerability in table partitioning was found in postgresql 10.x before 10.2, allowing an authenticated attacker to read arbitrary bytes of server memory via purpose-crafted insert to a partitioned table.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3381
2627	CVE-2018-1050	LOW	LOW	All versions of Samba from 4.0.0 onwards are vulnerable to a denial of service attack when the RPC spoolss service is configured to be run as an external daemon. Missing input sanitization checks on some of the input parameters to spoolss RPC calls could cause the print spooler service to crash.	samba	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3532
2628	CVE-2018-1049	MEDIUM	MEDIUM	In systemd prior to 234 a race condition exists between .mount and .automount units such that automount requests from kernel may not be serviced by systemd resulting in kernel holding the mountpoint and any processes that try to use said mount will hang. A race condition like this may lead to denial of service, until mount points are unmounted.	systemd	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3328
2629	CVE-2018-10393	MEDIUM	HIGH	bark_noise_hybridmp in psy.c in Xiph.Org libvorbis 1.3.6 has a stack-based buffer over-read.	libvorbis	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-3858
2630	CVE-2018-10392	MEDIUM	HIGH	mapping0_forward in mapping0.c in Xiph.Org libvorbis 1.3.6 does not validate the number of channels, which allows remote attackers to cause a denial of service (heap-based buffer overflow or over-read) or possibly have unspecified other impact via a crafted file.	libvorbis	Unchanged	8.0.0.27	9.0.0.17	10.17.41.8	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-3806
2631	CVE-2018-10373	MEDIUM	MEDIUM	concat_filename in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted binary file, as demonstrated by nm-new.	binutils	Unchanged	8.0.0.27	9.0.0.20	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3823
2632	CVE-2018-10372	MEDIUM	MEDIUM	process_cu_tu_index in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted binary file, as demonstrated by readelf.	binutils	Unchanged	8.0.0.27	9.0.0.20	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3834
2633	CVE-2018-10360	MEDIUM	MEDIUM	The do_core_note function in readelf.c in libmagic.a in file 5.33 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted ELF file.	file	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4101
2634	CVE-2018-10323	MEDIUM	MEDIUM	The xfs_bmap_extents_to_btree function in fs/xfs/libxfs/xfs_bmap.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service (xfs_bmapi_write NULL pointer dereference) via a crafted xfs image.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3819
2635	CVE-2018-10322	MEDIUM	MEDIUM	The xfs_dinode_verify function in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service (xfs_ilock_attr_map_shared invalid pointer dereference) via a crafted xfs image.	linux	Unchanged	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3844
2636	CVE-2018-10316	MEDIUM	MEDIUM	Netwide Assembler (NASM) 2.14rc0 has an endless while loop in the assemble_file function of asm/nasm.c because of a globallineno integer overflow.	nasm	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3799
2637	CVE-2018-10254	MEDIUM	HIGH	Netwide Assembler (NASM) 2.13 has a stack-based buffer over-read in the disasm function of the disasm/disasm.c file. Remote attackers could leverage this vulnerability to cause a denial of service or possibly have unspecified other impact via a crafted ELF file.	nasm	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	Investigate	Not vulnerable	Not vulnerable	LIN10-3833
2638	CVE-2018-10244	High	CRITICAL	Suricata version 4.0.4 incorrectly handles the parsing of an EtherNet/IP PDU. A malformed PDU can cause the parsing code to read beyond the allocated data because DecodeENIPPDU in app-layer-enip-commmon.c has an integer overflow during a length check.	suricata	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3847
2639	CVE-2018-10243	High	CRITICAL	htp_parse_authorization_digest in htp_parsers.c in LibHTP 0.5.26 allows remote attackers to cause a heap-based buffer over-read via an authorization digest header.	libhtp	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3852
2640	CVE-2018-10242	Medium	HIGH	Suricata version 4.0.4 incorrectly handles the parsing of the SSH banner. A malformed SSH banner can cause the parsing code to read beyond the allocated data because SSHParseBanner in app-layer-ssh.c lacks a length check.	suricata	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3848

	A	B	C	D	E	F	G	H	I	J	K	L	M
2641	CVE-2018-10195			Lrzsz has an integer overflow vulernability in the src/zm.c:zsdata() function. An attacker could exploit this with the sz command to cause a crash or potentially leak information to the receiving server.	lrzsz	Updated	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4857
2642	CVE-2018-10194	MEDIUM	HIGH	The set_text_distance function in devices/vector/gdevpdts.c in the pdfwrite component in Artifex Ghostscript through 9.22 does not prevent overflows in text-positioning calculation, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document.	ghostscript	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3808
2643	CVE-2018-10188	MEDIUM	HIGH	phpMyAdmin 4.8.0 before 4.8.0-1 has CSRF, allowing an attacker to execute arbitrary SQL statements, related to js/db_operations.js, js/tbl_operations.js, libraries/classes/Operations.php, and sql.php.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3861
2644	CVE-2018-10177	MEDIUM	MEDIUM	In ImageMagick 7.0.7-28, there is an infinite loop in the ReadOneMNGImage function of the coders/png.c file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted mng file.	imagemagick	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3835
2645	CVE-2018-10126	MEDIUM	MEDIUM	LibTIFF 4.0.9 has a NULL pointer dereference in the jpeg_fdct_16x16 function in jfdctint.c.	libtiff	Unchanged	Vulnerable	Vulnerable	Vulnerable	Investigate	Not vulnerable	Not vulnerable	LIN10-3850
2646	CVE-2018-10124	LOW	MEDIUM	The kill_something_info function in kernel/signal.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service via an INT_MIN argument.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3856
2647	CVE-2018-10114	MEDIUM	HIGH	An issue was discovered in GEGL through 0.3.32. The gegl_buffer_iterate_read_simple function in buffer/gegl-buffer-access.c allows remote attackers to cause a denial of service (write access violation) or possibly have unspecified other impact via a malformed PPM file, related to improper restrictions on memory allocation in the ppm_load_read_header function in operations/external/ppm-load.c.	gegl	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3839
2648	CVE-2018-10113	MEDIUM	HIGH	An issue was discovered in GEGL through 0.3.32. The process function in operations/external/ppm-load.c has unbounded memory allocation, leading to a denial of service (application crash) upon allocation failure.	gegl	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3821
2649	CVE-2018-10112	MEDIUM	HIGH	An issue was discovered in GEGL through 0.3.32. The gegl_tile_backend_swap_constructed function in buffer/gegl-tile-backend-swap.c allows remote attackers to cause a denial of service (write access violation) or possibly have unspecified other impact via a malformed PNG file that is mishandled during a call to the babl_format_get_bytes_per_pixel function in babl-format.c in babl 0.1.46.	gegl	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3809
2650	CVE-2018-10111	MEDIUM	HIGH	An issue was discovered in GEGL through 0.3.32. The render_rectangle function in process/gegl-processor.c has unbounded memory allocation, leading to a denial of service (application crash) upon allocation failure.	gegl	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3871
2651	CVE-2018-10105	High	CRITICAL	tcpdump before 4.9.3 mishandles the printing of SMB data (issue 2 of 2).	tcpdump	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN1018-4981
2652	CVE-2018-10103	High	CRITICAL	tcpdump before 4.9.3 mishandles the printing of SMB data (issue 1 of 2).	tcpdump	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	Not vulnerable	Not vulnerable	LIN1018-4980
2653	CVE-2018-10087	LOW	MEDIUM	The kernel_wait4 function in kernel/exit.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service by triggering an attempted use of the -INT_MIN value.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3802
2654	CVE-2018-10074	MEDIUM	MEDIUM	The hi3660_stub_clk_probe function in drivers/clk/hisilicon/clk-hi3660-stub.c in the Linux kernel before 4.16 allows local users to cause a denial of service (NULL pointer dereference) by triggering a failure of resource retrieval.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3749
2655	CVE-2018-1002209	MEDIUM	MEDIUM	QuaZIP before 0.7.6 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.	quazip	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9545
2656	CVE-2018-1002105	High	CRITICAL	In all Kubernetes versions prior to v1.10.11, v1.11.5, and v1.12.3, incorrect handling of error responses to proxied upgrade requests in the kube-apiserver allowed specially crafted requests to establish a connection through the Kubernetes API server to backend servers, then send arbitrary requests over the same connection directly to the backend, authenticated with the Kubernetes API server's TLS credentials used to establish the backend connection.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3259
2657	CVE-2018-1002100	LOW	MEDIUM	In Kubernetes versions 1.5.x, 1.6.x, 1.7.x, 1.8.x, and prior to version 1.9.6, the kubectl cp command insecurely handles tar data returned from the container, and can be caused to overwrite arbitrary local files.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4118
2658	CVE-2018-10021	MEDIUM	MEDIUM	drivers/scsi/libsas/sas_scsi_host.c in the Linux kernel before 4.16 allows local users to cause a denial of service (ata qc leak) by triggering certain failure conditions.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3721
2659	CVE-2018-10016	MEDIUM	MEDIUM	Netwide Assembler (NASM) 2.14rc0 has a division-by-zero vulnerability in the expr5 function in asm/eval.c via a malformed input file.	nasm	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3732
2660	CVE-2018-1000886	MEDIUM	MEDIUM	nasm version 2.14.01rc5, 2.15 contains a Buffer Overflow vulnerability in asm/stdscan.c:130 that can result in Stack-overflow caused by triggering endless macro generation, crash the program. This attack appear to be exploitable via a crafted nasm input file.	nasm	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Investigate	Investigate	LIN1018-3305
2661	CVE-2018-1000880	MEDIUM	MEDIUM	libarchive version commit 9693801580c0cf7c70e862d305270a16b52826a7 onwards (release v3.2.0 onwards) contains a CWE-20: Improper Input Validation vulnerability in WARC parser - libarchive/archive_read_support_format_warc.c, _warc_read() that can result in DoS - quasi-infinite run time and disk usage from tiny file. This attack appear to be exploitable via the victim must open a specially crafted WARC file.	libarchive	Unchanged	Not vulnerable	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3307

	A	B	C	D	E	F	G	H	I	J	K	L	M
2662	CVE-2018-1000879	MEDIUM	MEDIUM	libarchive version commit 379867ecb330b3a952fb7bfa7bffb7bbd5547205 onwards (release v3.3.0 onwards) contains a CWE-476: NULL Pointer Dereference vulnerability in ACL parser - libarchive/archive_acl.c, archive_acl_from_text_l() that can result in Crash/DoS. This attack appear to be exploitable via the victim must open a specially crafted archive file.	libarchive	Unchanged	Not vulnerable	Not vulnerable	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3329
2663	CVE-2018-1000878	MEDIUM	HIGH	libarchive version commit 41669491544921 9d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-416: Use After Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c that can result in Crash/DoS - it is unknown if RCE is possible. This attack appear to be exploitable via the victim must open a specially crafted RAR archive.	libarchive	Unchanged	8.0.0.29	Investigate	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3297
2664	CVE-2018-1000877	MEDIUM	HIGH	libarchive version commit 41669491544921 9d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-415: Double Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c, parse_codes(), realloc(rar->lzss.window, new_size) with new_size = 0 that can result in Crash/DoS. This attack appear to be exploitable via the victim must open a specially crafted RAR archive.	libarchive	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3304
2665	CVE-2018-1000876	MEDIUM	HIGH	binutils version 2.32 and earlier contains a Integer Overflow vulnerability in objdump, bfd_get_dynamic_reloc_upper_bound,bfd_canonicalize_dynamic_reloc that can result in Integer overflow trigger heap overflow. Successful exploitation allows execution of arbitrary code.. This attack appear to be exploitable via Local. This vulnerability appears to have been fixed in after commit 3a551c7a1b80fca579461774860574eabfd7f18f.	binutils	Unchanged	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3330
2666	CVE-2018-1000858	MEDIUM	HIGH	GnuPG version 2.1.12 - 2.2.11 contains a Cross ite Request Forgery (CSRF) vulnerability in dirmngr that can result in Attacker controlled CSRF, Information Disclosure, DoS. This attack appear to be exploitable via Victim must perform a WKD request, e.g. enter an email address in the composer window of Thunderbird/Enigmail. This vulnerability appears to have been fixed in after commit 4a4bb874f63741026bd26264c43bb32b1099f060.	gnupg	Unchanged	Vulnerable	Vulnerable	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3340
2667	CVE-2018-1000852	HIGH	CRITICAL	FreeRDP FreeRDP 2.0.0-rc3 released version before commit 205c612820dac644d665b5bb1cdf437dc5ca01e3 contains a Other/Unknown vulnerability in channels/drdynvc/client/drdynvc_main.c, drdynvc_process_capability_request that can result in The RDP server can read the client's memory.. This attack appear to be exploitable via RDPClient must connect the rdp server with echo option. This vulnerability appears to have been fixed in after commit 205c612820dac644d665b5bb1cdf437dc5ca01e3.	freerdp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3331
2668	CVE-2018-1000845			Avahi version 0.7 contains a Incorrect Access Control vulnerability in avahi-daemon that can result in Traffic reflection and amplification for DDoS attacks.. This attack appear to be exploitable via unicast IP network packet with spoofed source address.	avahi	Updated	8.0.0.29	9.0.0.20	10.17.41.14	10.18.44.3	Not vulnerable	Not vulnerable	LIN1018-3341
2669	CVE-2018-1000802	HIGH	CRITICAL	Python Software Foundation Python (CPython) version 2.7 contains a CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in shutil module (make_archive function) that can result in Denial of service, Information gain via injection of arbitrary files on the system or entire drive. This attack appear to be exploitable via Passage of unfiltered user input to the function. This vulnerability appears to have been fixed in after commit add531a1e55b0a739b0f42582f1c9747e5649ace.	python	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4799
2670	CVE-2018-1000667	MEDIUM	MEDIUM	NASM nasm-2.13.03 nasm- 2.14rc15 version 2.14rc15 and earlier contains a memory corruption (crashed) of nasm when handling a crafted file due to function assemble_file(inname, depend_ptr) at asm/nasm.c:482. vulnerability in function assemble_file(inname, depend_ptr) at asm/nasm.c:482. that can result in aborting/crash nasm program. This attack appear to be exploitable via a specially crafted asm file..	nasm	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4694
2671	CVE-2018-1000654	HIGH	MEDIUM	GNU Libtasn1-4.13 libtasn1-4.13 version libtasn1-4.13, libtasn1-4.12 contains a DoS, specifically CPU usage will reach 100% when running asn1Paser against the POC due to an issue in _asn1_expand_object_id(p_tree), after a long time, the program will be killed. This attack appears to be exploitable via parsing a crafted file.	libtasn1	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Vulnerable	LIN10-4590
2672	CVE-2018-1000632	MEDIUM	HIGH	dom4j version prior to version 2.1.1 contains a CWE-91: XML Injection vulnerability in Class: Element. Methods: addElement, addAttribute that can result in an attacker tampering with XML documents through XML injection. This attack appear to be exploitable via an attacker specifying attributes or elements in the XML document. This vulnerability appears to have been fixed in 2.1.1 or later.	dom4j	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9708
2673	CVE-2018-1000536	MEDIUM	MEDIUM	Medis version 0.6.1 and earlier contains a XSS vulnerability evolving into code execution due to enabled nodeIntegration for the renderer process vulnerability in Key name parameter on new key creation that can result in Unauthorized code execution in the victim's machine, within the rights of the running application. This attack appear to be exploitable via Victim is synchronizing data from the redis server which contains malicious key value.	redis	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4232

	A	B	C	D	E	F	G	H	I	J	K	L	M
2674	CVE-2018-1000520	MEDIUM	HIGH	ARM mbedTLS version 2.7.0 and earlier contains a Ciphersuite Allows Incorrectly Signed Certificates vulnerability in mbedtls_ssl_get_verify_result() that can result in ECDSA-signed certificates are accepted, when only RSA-signed ones should be.. This attack appear to be exploitable via Peers negotiate a TLS-ECDH-RSA-* ciphersuite. Any of the peers can then provide an ECDSA-signed certificate, when only an RSA-signed one should be accepted..	mbedtls	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4223
2675	CVE-2018-1000517	HIGH	CRITICAL	BusyBox project BusyBox wget version prior to commit 8e2174e9bd836e53c8b9c6e00d1bc6e2a718686e contains a Buffer Overflow vulnerability in Busybox wget that can result in heap buffer overflow. This attack appear to be exploitable via network connectivity. This vulnerability appears to have been fixed in after commit 8e2174e9bd836e53c8b9c6e00d1bc6e2a718686e.	busybox	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4208
2676	CVE-2018-1000500	MEDIUM	HIGH	Busybox contains a Missing SSL certificate validation vulnerability in The busybox wget applet that can result in arbitrary code execution. This attack appear to be exploitable via Simply download any file over HTTPS using busybox wget https://compromised-domain.com/important-file.	busybox	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4213
2677	CVE-2018-1000301	MEDIUM	CRITICAL	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in denial of service that can result in curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP content.. This vulnerability appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.	curl	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4055
2678	CVE-2018-1000300	HIGH	CRITICAL	curl version curl 7.54.1 to and including curl 7.59.0 contains a CWE-122: Heap-based Buffer Overflow vulnerability in denial of service and more that can result in curl might overflow a heap based memory buffer when closing down an FTP connection with very long server command replies.. This vulnerability appears to have been fixed in curl < 7.54.1 and curl >= 7.60.0.	curl	Unchanged	Not vulnerable	Not vulnerable	10.17.41.9	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4033
2679	CVE-2018-1000222	MEDIUM	HIGH	Libgd version 2.2.5 contains a Double Free Vulnerability vulnerability in gdImageBmpPtr Function that can result in Remote Code Execution . This attack appear to be exploitable via Specially Crafted Jpeg Image can trigger double free. This vulnerability appears to have been fixed in after commit ac16bdf2d41724b5a65255d4c28fb0ec46bc42f5.	gd	Unchanged	8.0.0.28	9.0.0.18	10.17.41.12	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-4637
2680	CVE-2018-1000221	HIGH	CRITICAL	pkgconf version 1.5.0 to 1.5.2 contains a Buffer Overflow vulnerability in dequote() that can result in dequote() function returns 1-byte allocation if initial length is 0, leading to buffer overflow. This attack appear to be exploitable via specially crafted .pc file. This vulnerability appears to have been fixed in 1.5.3.	pkgconf	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4601
2681	CVE-2018-1000205	MEDIUM	MEDIUM	U-Boot contains a CWE-20: Improper Input Validation vulnerability in Verified boot signature validation that can result in Bypass verified boot. This attack appear to be exploitable via Specially crafted FIT image and special device memory functionality.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4207
2682	CVE-2018-1000204	MEDIUM	MEDIUM	Linux Kernel version 3.18 to 4.16 incorrectly handles an SG_IO ioctl on /dev/sg0 with dxfer_direction=SG_DXFER_FROM_DEV and an empty 6-byte cmdp. This may lead to copying up to 1000 kernel heap pages to the userspace. This has been fixed upstream already: https://github.com/torvalds/linux/commit/a45b599ad808c3c982fdcdc12b0b8611c2f92824 The problem has limited scope, as users don't usually have permissions to access SCSI devices. On the other hand, e.g. the Nero user manual suggests doing `chmod o+r+w /dev/sg*` to make the devices accessible.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4224
2683	CVE-2018-1000200	MEDIUM	MEDIUM	The Linux Kernel versions 4.14, 4.15, and 4.16 has a null pointer dereference which can result in an out of memory (OOM) killing of large mlocked processes. The issue arises from an oom killed process's final thread calling exit_mmap(), which calls munlock_vma_pages_all() for mlocked vmas.This can happen synchronously with the oom reaper's unmap_page_range() since the vma's VM_LOCKED bit is cleared before munlocking (to determine if any other vmas share the memory and are mlocked).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4102
2684	CVE-2018-1000199	MEDIUM	MEDIUM	The Linux Kernel version 3.18 contains a dangerous feature vulnerability in modify_user_hw_breakpoint() that can result in crash and possibly memory corruption. This attack appear to be exploitable via local code execution and the ability to use ptrace. This vulnerability appears to have been fixed in git commit f67b15037a7a50c57f72e69a6d59941ad90a0f0f.	linux	Unchanged	8.0.0.27	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4043
2685	CVE-2018-1000168	MEDIUM	HIGH	nghttp2 version >= 1.10.0 and nghttp2 <= v1.31.0 contains an Improper Input Validation CWE-20 vulnerability in ALTSVC frame handling that can result in segmentation fault leading to denial of service. This attack appears to be exploitable via network client. This vulnerability appears to have been fixed in >= 1.31.1.	nghttp2	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3934
2686	CVE-2018-1000164	MEDIUM	HIGH	gunicorn version 19.4.5 contains a CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers vulnerability in process_headers function in gunicorn/http/wsgi.py that can result in an attacker causing the server to return arbitrary HTTP headers. This vulnerability appears to have been fixed in 19.5.0.	gunicorn	Unchanged	8.0.0.26	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3855

	A	B	C	D	E	F	G	H	I	J	K	L	M
2687	CVE-2018-1000161	LOW	MEDIUM	nmap version 6.49BETA6 through 7.60, up to and including SVN revision 37147 contains a Directory Traversal vulnerability in NSE script http-fetch that can result in file overwrite as the user is running it. This attack appears to be exploitable via a victim that runs NSE script http-fetch against a malicious web site. This vulnerability appears to have been fixed in 7.7.	nmap	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3837
2688	CVE-2018-1000156	MEDIUM	HIGH	GNU Patch version 2.7.6 contains an input validation vulnerability when processing patch files, specifically the EDITOR_PROGRAM invocation (using ed) can result in code execution. This attack appear to be exploitable via a patch file processed via the patch utility. This is similar to FreeBSD's CVE-2015-1418 however although they share a common ancestry the code bases have diverged over time.	patch	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3687
2689	CVE-2018-1000155	HIGH	CRITICAL	OpenFlow version 1.0 onwards contains a Denial of Service and Improper authorization vulnerability in OpenFlow handshake: The DPID (DataPath IDentifier) in the features_reply message are inherently trusted by the controller. that can result in Denial of Service, Unauthorized Access, Network Instability. This attack appear to be exploitable via Network connectivity: the attacker must first establish a transport connection with the OpenFlow controller and then initiate the OpenFlow handshake.	openflow	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4057
2690	CVE-2018-1000140	HIGH	CRITICAL	rsyslog librelp version 1.2.14 and earlier contains a Buffer Overflow vulnerability in the checking of x509 certificates from a peer that can result in Remote code execution. This attack appear to be exploitable a remote attacker that can connect to rsyslog and trigger a stack buffer overflow by sending a specially crafted x509 certificate.	rsyslog&librelp	Unchanged	Not vulnerable	9.0.0.16	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3642
2691	CVE-2018-1000132	MEDIUM	CRITICAL	Mercurial version 4.5 and earlier contains a Incorrect Access Control (CWE-285) vulnerability in Protocol server that can result in Unauthorized data access. This attack appear to be exploitable via network connectivity. This vulnerability appears to have been fixed in 4.5.1.	mercurial	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3525
2692	CVE-2018-1000127	MEDIUM	HIGH	memcached version prior to 1.4.37 contains an Integer Overflow vulnerability in items.c:item_free() that can result in data corruption and deadlocks due to items existing in hash table being reused from free list. This attack appear to be exploitable via network connectivity to the memcached service. This vulnerability appears to have been fixed in 1.4.37 and later.	memcached	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3557
2693	CVE-2018-1000122	MEDIUM	CRITICAL	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage	curl	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3555
2694	CVE-2018-1000121	MEDIUM	HIGH	A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an attacker to cause a denial of service	curl	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3580
2695	CVE-2018-1000120	HIGH	CRITICAL	A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause a denial of service or worse.	curl	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3549
2696	CVE-2018-1000117	HIGH	MEDIUM	Python Software Foundation CPython version From 3.2 until 3.6.4 on Windows contains a Buffer Overflow vulnerability in os.symlink() function on Windows that can result in Arbitrary code execution, likely escalation of privilege. This attack appears to be exploitable via a python script that creates a symlink with an attacker controlled name or location. This vulnerability appears to have been fixed in 3.7.0 and 3.6.5.	python	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3506
2697	CVE-2018-1000116	HIGH	CRITICAL	NET-SNMP version 5.7.2 contains a heap corruption vulnerability in the UDP protocol handler that can result in command execution.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3576
2698	CVE-2018-1000115	MEDIUM	HIGH	Memcached version 1.5.5 contains an Insufficient Control of Network Message Volume (Network Amplification, CWE-406) vulnerability in the UDP support of the memcached server that can result in denial of service via network flood (traffic amplification of 1:50,000 has been reported by reliable sources). This attack appear to be exploitable via network connectivity to port 11211 UDP. This vulnerability appears to have been fixed in 1.5.6 due to the disabling of the UDP protocol by default.	memcached	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3522
2699	CVE-2018-10001	MEDIUM	MEDIUM	The decode_init function in libavcodec/utvideodec.c in FFmpeg through 3.4.2 allows remote attackers to cause a denial of service (out of array read) via an AVI file.	ffmpeg	Unchanged	Not vulnerable	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3731
2700	CVE-2018-1000097	MEDIUM	HIGH	Sharutils sharutils (unshar command) version 4.15.2 contains a Buffer Overflow vulnerability in Affected component on the file unshar.c at line 75, function looks_like_c_code. Failure to perform checking of the buffer containing input line. that can result in Could lead to code execution. This attack appear to be exploitable via Victim have to run unshar command on a specially crafted file..	sharutils	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3524
2701	CVE-2018-1000085	MEDIUM	MEDIUM	ClamAV version version 0.99.3 contains a Out of bounds heap memory read vulnerability in XAR parser, function xar_hash_check() that can result in Leaking of memory, may help in developing exploit chains.. This attack appear to be exploitable via The victim must scan a crafted XAR file. This vulnerability appears to have been fixed in after commit d96a6b9bcc7439fa7e3876207aa0a8e79c8451b6.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3512
2702	CVE-2018-1000079	MEDIUM	MEDIUM	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Directory Traversal vulnerability in gem installation that can result in the gem could write to arbitrary filesystem locations during installation. This attack appear to be exploitable via the victim must install a malicious gem. This vulnerability appears to have been fixed in 2.7.6.	ruby	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3511

	A	B	C	D	E	F	G	H	I	J	K	L	M
2703	CVE-2018-1000078	MEDIUM	MEDIUM	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Cross Site Scripting (XSS) vulnerability in gem server display of homepage attribute that can result in XSS. This attack appear to be exploitable via the victim must browse to a malicious gem on a vulnerable gem server. This vulnerability appears to have been fixed in 2.7.6.	ruby	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3583
2704	CVE-2018-1000077	MEDIUM	MEDIUM	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Improper Input Validation vulnerability in ruby gems specification homepage attribute that can result in a malicious gem could set an invalid homepage URL. This vulnerability appears to have been fixed in 2.7.6.	ruby	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3518
2705	CVE-2018-1000076	HIGH	CRITICAL	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Improper Verification of Cryptographic Signature vulnerability in package.rb that can result in a mis-signed gem could be installed, as the tarball would contain multiple gem signatures.. This vulnerability appears to have been fixed in 2.7.6.	ruby	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3545
2706	CVE-2018-1000075	MEDIUM	HIGH	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a infinite loop caused by negative size vulnerability in ruby gem package tar header that can result in a negative size could cause an infinite loop.. This vulnerability appears to have been fixed in 2.7.6.	ruby	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3527
2707	CVE-2018-1000074	MEDIUM	HIGH	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Deserialization of Untrusted Data vulnerability in owner command that can result in code execution. This attack appear to be exploitable via victim must run the `gem owner` command on a gem with a specially crafted YAML file. This vulnerability appears to have been fixed in 2.7.6.	ruby	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3551
2708	CVE-2018-1000073	MEDIUM	HIGH	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Directory Traversal vulnerability in install_location function of package.rb that can result in path traversal when writing to a symlinked basedir outside of the root. This vulnerability appears to have been fixed in 2.7.6.	ruby	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3537
2709	CVE-2018-1000061	HIGH	CRITICAL	ARM mbedTLS version development branch, 2.7.0 and earlier contains a CWE-670, Incorrect condition control flow leading to incorrect return, leading to data loss vulnerability in ssl_write_real(), library/ssl_tls.c:7142 that can result in Leads to data loss, can be escalated to DoS and authorization bypass in application protocols. This attack appear to be exploitable via network connectivity.	mbedtls	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3355
2710	CVE-2018-1000041	MEDIUM	HIGH	GNOME librsvg version before commit c6ddf2ed4d768fd88adbea2b63f575cd523022ea contains a Improper input validation vulnerability in rsvg-io.c that can result in the victim's Windows username and NTLM password hash being leaked to remote attackers through SMB. This attack appear to be exploitable via The victim must process a specially crafted SVG file containing an UNC path on Windows.	librsvg	Unchanged	8.0.0.27	9.0.0.17	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3326
2711	CVE-2018-1000035	MEDIUM	HIGH	A heap-based buffer overflow exists in Info-Zip UnZip version <= 6.00 in the processing of password-protected archives that allows an attacker to perform a denial of service or to possibly achieve code execution.	unzip	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-3407
2712	CVE-2018-1000034	MEDIUM	CRITICAL	An out-of-bounds read exists in Info-Zip UnZip version 6.10c22 that allows an attacker to perform a denial of service and read sensitive memory.	unzip	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3345
2713	CVE-2018-1000033	MEDIUM	CRITICAL	An out-of-bounds read exists in Info-Zip UnZip version 6.10c22 that allows an attacker to perform a denial of service and read sensitive memory.	unzip	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3314
2714	CVE-2018-1000032	MEDIUM	HIGH	A heap-based buffer overflow exists in Info-Zip UnZip version 6.10c22 that allows an attacker to perform a denial of service or to possibly achieve code execution.	unzip	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3397
2715	CVE-2018-1000031	MEDIUM	HIGH	A heap-based buffer overflow exists in Info-Zip UnZip version 6.10c22 that allows an attacker to perform a denial of service or to possibly achieve code execution.	unzip	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3385

	A	B	C	D	E	F	G	H	I	J	K	L	M
2716	CVE-2018-1000030	MEDIUM	HIGH	Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions prior to 2.7.14 may also be vulnerable and it appears that Python 2.7.17 and prior may also be vulnerable however this has not been confirmed. The vulnerability lies when multiply threads are handling large amounts of data. In both cases there is essentially a race condition that occurs. For the Heap-Buffer-Overflow, Thread 2 is creating the size for a buffer, but Thread1 is already writing to the buffer without knowing how much to write. So when a large amount of data is being processed, it is very easy to cause memory corruption using a Heap-Buffer-Overflow. As for the Use-After-Free, Thread3->Malloc->Thread1->Free's->Thread2-Re-uses-Free'd Memory. The PSRT has stated that this is not a security vulnerability due to the fact that the attacker must be able to run code, however in some situations, such as function as a service, this vulnerability can potentially be used by an attacker to violate a trust boundary, as such the DWF feels this issue deserves a CVE.	python	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3420
2717	CVE-2018-1000028	MEDIUM	HIGH	Linux kernel version after commit bdcf0a423ea1 - 4.15-rc4+, 4.14.8+, 4.9.76+, 4.4.111+ contains a Incorrect Access Control vulnerability in NFS server (nfsd) that can result in remote users reading or writing files they should not be able to via NFS. This attack appear to be exploitable via NFS server must export a filesystem with the rootsquash options enabled. This vulnerability appears to have been fixed in after commit 1995266727fa.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3439
2718	CVE-2018-1000026	MEDIUM	HIGH	Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation vulnerability in bnx2x network card driver that can result in DoS: Network card firmware assertion takes card off-line. This attack appear to be exploitable via An attacker on a must pass a very large, specially crafted packet to the bnx2x card. This can be done from an untrusted guest VM..	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3318
2719	CVE-2018-1000021	MEDIUM	HIGH	GIT version 2.15.1 and earlier contains a Input Validation Error vulnerability in Client that can result in problems including messing up terminal configuration to RCE. This attack appear to be exploitable via The user must interact with a malicious git server, (or have their traffic modified in a MITM attack).	git	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3423
2720	CVE-2018-1000007	MEDIUM	CRITICAL	libcurl 7.1 through 7.57.0 might accidentally leak authentication data to third parties. When asked to send custom headers in its HTTP requests, libcurl will send that set of headers first to the host in the initial URL but also, if asked to follow redirects and a 30X HTTP response code is returned, to the host mentioned in URL in the `Location:` response header value. Sending the same set of headers to subsequest hosts is in particular a problem for applications that pass on custom `Authorization:` headers, as this header often contains privacy sensitive information or data that could allow others to impersonate the libcurl-using client's request.	curl	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3225
2721	CVE-2018-1000005	MEDIUM	CRITICAL	libcurl 7.49.0 to and including 7.57.0 contains an out bounds read in code handling HTTP/2 trailers. It was reported (https://github.com/curl/curl/pull/2231) that reading an HTTP/2 trailer could mess up future trailers since the stored size was one byte less than required. The problem is that the code that creates HTTP/1-like headers from the HTTP/2 trailer data once appended a string like `:` to the target buffer, while this was recently changed to `: ` (a space was added after the colon) but the following math wasn't updated correspondingly. When accessed, the data is read out of bounds and causes either a crash or that the (too large) data gets passed to client write. This could lead to a denial-of-service situation or an information disclosure if someone has a service that echoes back or uses the trailers for something.	curl	Unchanged	Not vulnerable	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3221
2722	CVE-2018-1000004	HIGH	MEDIUM	In the Linux kernel 4.12, 3.10, 2.6 and possibly earlier versions a race condition vulnerability exists in the sound system, this can lead to a deadlock and denial of service condition.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3229
2723	CVE-2018-1000001	High	High	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.	glibc	Unchanged	8.0.0.26	9.0.0.15	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3344
2724	CVE-2018-0739	MEDIUM	MEDIUM	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).	openssl	Unchanged	8.0.0.26	9.0.0.16	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3640
2725	CVE-2018-0737	MEDIUM	MEDIUM	The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).	openssl	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3832
2726	CVE-2018-0735	MEDIUM	MEDIUM	The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.0j-dev (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.1.1a-dev (Affected 1.1.1).	openssl	Unchanged	Not vulnerable	Not vulnerable	10.17.41.13	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4907

	A	B	C	D	E	F	G	H	I	J	K	L	M
2727	CVE-2018-0734	MEDIUM	MEDIUM	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a-dev (Affected 1.1.1). Fixed in OpenSSL 1.1.0j-dev (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q-dev (Affected 1.0.2-1.0.2p).	openssl	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.3	Not vulnerable	Vulnerable	LIN10-4890
2728	CVE-2018-0733	MEDIUM	MEDIUM	Because of an implementation bug the PA-RISC CRYPTO_memcmp function is effectively reduced to only comparing the least significant bit of each byte. This allows an attacker to forge messages that would be considered as authenticated in an amount of tries lower than that guaranteed by the security claims of the scheme. The module can only be compiled by the HP-UX assembler, so that only HP-UX PA-RISC targets are affected. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g).	openssl	Unchanged	Not vulnerable	Not vulnerable	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3680
2729	CVE-2018-0732	MEDIUM	HIGH	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).	openssl	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4109
2730	CVE-2018-0502	HIGH	CRITICAL	An issue was discovered in zsh before 5.6. The beginning of a #! script file was mishandled, potentially leading to an execve call to a program named on the second line.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4717
2731	CVE-2018-0500	HIGH	CRITICAL	Curl_smtp_escape_eob in lib/smtp.c in curl before 7.61.0 has a heap-based buffer overflow that might be exploitable by an attacker who can control the data that curl transmits over SMTP with certain settings (i.e., use of a nonstandard --limit-rate argument or CURLOPT_BUFFERSIZE value).	curl	Unchanged	Not vulnerable	Not vulnerable	10.17.41.10	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4299
2732	CVE-2018-0498	LOW	MEDIUM	ARM mbed TLS before 2.12.0, before 2.7.5, and before 2.1.14 allows local users to achieve partial plaintext recovery (for a CBC based ciphersuite) via a cache-based side-channel attack.	mbedtls	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4410
2733	CVE-2018-0497	MEDIUM	MEDIUM	ARM mbed TLS before 2.12.0, before 2.7.5, and before 2.1.14 allows remote attackers to achieve partial plaintext recovery (for a CBC based ciphersuite) via a timing-based side-channel attack. This vulnerability exists because of an incorrect fix (with a wrong SHA-384 calculation) for CVE-2013-0169.	mbedtls	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4436
2734	CVE-2018-0495	LOW	MEDIUM	Libgcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can be mitigated through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ecdsa.c, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.	libgcrypt	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4106
2735	CVE-2018-0494	MEDIUM	MEDIUM	GNU Wget before 1.19.5 is prone to a cookie injection vulnerability in the resp_new function in http.c via a \r\n sequence in a continuation line.	wget	Unchanged	Not vulnerable	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3939
2736	CVE-2018-0488	HIGH	CRITICAL	ARM mbed TLS before 1.3.22, before 2.1.10, and before 2.7.0, when the truncated HMAC extension and CBC are used, allows remote attackers to execute arbitrary code or cause a denial of service (heap corruption) via a crafted application packet within a TLS or DTLS session.	mbedtls	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3365
2737	CVE-2018-0487	HIGH	CRITICAL	ARM mbed TLS before 1.3.22, before 2.1.10, and before 2.7.0 allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow) via a crafted certificate chain that is mishandled during RSASSA-PSS signature verification within a TLS or DTLS session.	mbedtls	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3361
2738	CVE-2018-0361	MEDIUM	LOW	ClamAV before 0.100.1 lacks a PDF object length check, resulting in an unreasonably long time to parse a relatively small file.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4388
2739	CVE-2018-0360	MEDIUM	MEDIUM	ClamAV before 0.100.1 has an HWP integer overflow with a resultant infinite loop via a crafted Hangul Word Processor file. This is in parsehwp3_paragraph() in libclamav/hwp.c.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4467
2740	CVE-2018-0202	MEDIUM	MEDIUM	clamscan in ClamAV before 0.99.4 contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation checking mechanisms when handling Portable Document Format (.pdf) files sent to an affected device. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted .pdf file to an affected device. This action could cause an out-of-bounds read when ClamAV scans the malicious file, allowing the attacker to cause a DoS condition. This concerns pdf_parse_array and pdf_parse_string in libclamav/pdfng.c. Cisco Bug IDs: CSCvh91380, CSCvh91400.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3673
2741	CVE-2017-9996	MEDIUM	High	The cdxl_decode_frame function in libavcodec/cdxl.c in FFmpeg 2.8.x before 2.8.12, 3.0.x before 3.0.8, 3.1.x before 3.1.8, 3.2.x before 3.2.5, and 3.3.x before 3.3.1 does not exclude the CHUNKY format, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file.	ffmpeg	Unchanged	Won't Fix	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4544
2742	CVE-2017-9995	MEDIUM	High	libavcodec/scpr.c in FFmpeg 3.3 before 3.3.1 does not properly validate height and width data, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4490

	A	B	C	D	E	F	G	H	I	J	K	L	M
2743	CVE-2017-9994	MEDIUM	High	libavcodec/webp.c in FFmpeg before 2.8.12, 3.0.x before 3.0.8, 3.1.x before 3.1.8, 3.2.x before 3.2.5, and 3.3.x before 3.3.1 does not ensure that pix_fmt is set, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file, related to the vp8_decode_mb_row_no_filter and pred8x8_128_dc_8_c functions.	ffmpeg	Unchanged	Won't Fix	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4526
2744	CVE-2017-9993	MEDIUM	High	FFmpeg before 2.8.12, 3.0.x and 3.1.x before 3.1.9, 3.2.x before 3.2.6, and 3.3.x before 3.3.2 does not properly restrict HTTP Live Streaming filename extensions and demuxer names, which allows attackers to read arbitrary files via crafted playlist data.	ffmpeg	Unchanged	Won't Fix	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4517
2745	CVE-2017-9992	MEDIUM	High	Heap-based buffer overflow in the decode_dds1 function in libavcodec/dfa.c in FFmpeg before 2.8.12, 3.0.x before 3.0.8, 3.1.x before 3.1.8, 3.2.x before 3.2.5, and 3.3.x before 3.3.1 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file.	ffmpeg	Unchanged	Won't Fix	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4499
2746	CVE-2017-9991	MEDIUM	High	Heap-based buffer overflow in the xwd_decode_frame function in libavcodec/xwddec.c in FFmpeg before 2.8.12, 3.0.x before 3.0.8, 3.1.x before 3.1.8, 3.2.x before 3.2.5, and 3.3.x before 3.3.1 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file.	ffmpeg	Unchanged	Won't Fix	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4568
2747	CVE-2017-9990	MEDIUM	High	Stack-based buffer overflow in the color_string_to_rgba function in libavcodec/xpmdec.c in FFmpeg 3.3 before 3.3.1 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4529
2748	CVE-2017-9987	MEDIUM	High	There is a heap-based buffer overflow in the function hpel_motion in mpegvideo_motion.c in libav 12.1. A crafted input can lead to a remote denial of service attack.	libav	Unchanged	Vulnerable	Vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4494
2749	CVE-2017-9986	HIGH	High	The intr function in sound/oss/msnd_pinnacle.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer between two kernel reads of that value, aka a double fetch vulnerability.	linux	Unchanged	8.0.0.21	9.0.0.10	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4538
2750	CVE-2017-9985	HIGH	High	The snd_msndmidi_input_read function in sound/isa/msnd/msnd_midi.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer between two kernel reads of that value, aka a double fetch vulnerability.	linux	Unchanged	8.0.0.21	9.0.0.10	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4511
2751	CVE-2017-9984	HIGH	High	The snd_msnd_interrupt function in sound/isa/msnd/msnd_pinnacle.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer between two kernel reads of that value, aka a double fetch vulnerability.	linux	Unchanged	8.0.0.21	9.0.0.10	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4491
2752	CVE-2017-9955	MEDIUM	Medium	The get_build_id function in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file in which a certain size field is larger than a corresponding data field, as demonstrated by mishandling within the objdump program.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4506
2753	CVE-2017-9954	MEDIUM	Medium	The getvalue function in tekhex.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a crafted tekhex file, as demonstrated by mishandling within the nm program.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4564
2754	CVE-2017-9951	MEDIUM	High	The try_read_command function in memcached.c in memcached before 1.4.39 allows remote attackers to cause a denial of service (segmentation fault) via a request to add/set a key, which makes a comparison between signed and unsigned int and triggers a heap-based buffer over-read. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8705.	memcached	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4753
2755	CVE-2017-9937	MEDIUM	Medium	In LibTIFF 4.0.8, there is a memory malloc failure in tif_jbig.c. A crafted TIFF document can lead to an abort resulting in a remote denial of service attack.	libtiff	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-4567
2756	CVE-2017-9936	MEDIUM	Medium	In LibTIFF 4.0.8, there is a memory leak in tif_jbig.c. A crafted TIFF document can lead to a memory leak resulting in a remote denial of service attack.	libtiff	Unchanged	8.0.0.19	9.0.0.8	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-4501
2757	CVE-2017-9935	MEDIUM	High	In LibTIFF 4.0.8, there is a heap-based buffer overflow in the t2p_write_pdf function in tools/tiff2pdf.c. This heap overflow could lead to different damages. For example, a crafted TIFF document can lead to an out-of-bounds read in TIFFCleanup, an invalid free in TIFFClose or t2p_free, memory corruption in t2p_readwrite_pdf_image, or a double free in t2p_free. Given these possibilities, it probably could cause arbitrary code execution.	libtiff	Unchanged	8.0.0.25	9.0.0.15	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-4493
2758	CVE-2017-9872	MEDIUM	High	The III_dequantize_sample function in layer3.c in mpglib, as used in libmpgdecoder.a in LAME 3.99.5 and other products, allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted audio file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4514

	A	B	C	D	E	F	G	H	I	J	K	L	M
2759	CVE-2017-9871	MEDIUM	High	The III_i_stereo function in layer3.c in mpglib, as used in libmpgdecoder.a in LAME 3.99.5 and other products, allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted audio file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4542
2760	CVE-2017-9870	MEDIUM	Medium	The III_i_stereo function in layer3.c in mpglib, as used in libmpgdecoder.a in LAME 3.99.5 and other products, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4533
2761	CVE-2017-9869	MEDIUM	Medium	The II_step_one function in layer2.c in mpglib, as used in libmpgdecoder.a in LAME 3.99.5 and other products, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4510
2762	CVE-2017-9865	MEDIUM	Medium	The function GfxImageColorMap::getGray in GfxState.cc in Poppler 0.54.0 allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a crafted PDF document, related to missing color-map validation in ImageOutputDev.cc.	poppler	Unchanged	Won't Fix	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4561
2763	CVE-2017-9847	MEDIUM	Medium	The bdecode function in bdecode.cpp in libtorrent 1.1.3 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file.	libtorrent	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4552
2764	CVE-2017-9835	MEDIUM	High	The gs_alloc_ref_array function in psi/ialloc.c in Artifex Ghostscript 9.22 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PostScript document. This is related to a lack of an integer overflow check in base/gsalloc.c.	ghostscript	Unchanged	8.0.0.21	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4809
2765	CVE-2017-9832	MEDIUM	Medium	An integer overflow vulnerability in ptp-pack.c (ptp_unpack_OPL function) of libmtp (version 1.1.12 and below) allows attackers to cause a denial of service (out-of-bounds memory access) or maybe remote code execution by inserting a mobile device into a personal computer through a USB cable.	libmtp	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4492
2766	CVE-2017-9831	MEDIUM	Medium	An integer overflow vulnerability in the ptp_unpack_EOS_CustomFuncEx function of the ptp-pack.c file of libmtp (version 1.1.12 and below) allows attackers to cause a denial of service (out-of-bounds memory access) or maybe remote code execution by inserting a mobile device into a personal computer through a USB cable.	libmtp	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4539
2767	CVE-2017-9815	MEDIUM	Medium	In LibTIFF 4.0.7, the TIFFReadDirEntryLong8Array function in libtiff/tif_dirread.c mishandles a malloc operation, which allows attackers to cause a denial of service (memory leak within the function _TIFFmalloc in tif_unix.c) via a crafted file.	libtiff	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4521
2768	CVE-2017-9814	Medium	High	cairo-truetype-subset.c in cairo 1.15.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) because of mishandling of an unexpected malloc(0) call.	cairo	Unchanged	8.0.0.30	9.0.0.21	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-4839
2769	CVE-2017-9800	HIGH	Critical	A maliciously constructed svn+ssh:// URL would cause Subversion clients before 1.8.19, 1.9.x before 1.9.7, and 1.10.0.x through 1.10.0-alpha3 to run an arbitrary shell command. Such a URL could be generated by a malicious server, by a malicious user committing to a honest server (to attack another user of that server's repositories), or by a proxy server. The vulnerability affects all clients, including those that use file://, http://, and plain (untunneled) svn://.	subversion	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5151
2770	CVE-2017-9798	MEDIUM	High	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.	apache2	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5474
2771	CVE-2017-9789	Medium	High	When under stress, closing many connections, the HTTP/2 handling code in Apache httpd 2.4.26 would sometimes access memory after it has been freed, resulting in potentially erratic behaviour.	apache2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4851
2772	CVE-2017-9788	Medium	Critical	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.	apache2	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4795
2773	CVE-2017-9782	MEDIUM	Medium	JasPer 2.0.12 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted image, related to the jp2_decode function in libjasper/jp2/jp2_dec.c.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4556
2774	CVE-2017-9778	MEDIUM	Medium	GNU Debugger (GDB) 8.0 and earlier fails to detect a negative length field in a DWARF section. A malformed section in an ELF binary or a core file can cause GDB to repeatedly allocate memory until a process limit is reached. This can, for example, impede efforts to analyze malware with GDB.	gdb	Unchanged	8.0.0.31	9.0.0.24	10.17.41.20	10.18.44.12	10.19.45.1	Not vulnerable	LIN9-4566

	A	B	C	D	E	F	G	H	I	J	K	L	M
2775	CVE-2017-9776	MEDIUM	High	Integer overflow leading to Heap buffer overflow in JBIG2Stream.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document.	poppler	Unchanged	Won't Fix	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4551
2776	CVE-2017-9775	MEDIUM	Medium	Stack buffer overflow in GfxState.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) via a crafted PDF document.	poppler	Unchanged	Won't Fix	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4562
2777	CVE-2017-9766	MEDIUM	High	In Wireshark 2.2.7, PROFINET IO data with a high recursion depth allows remote attackers to cause a denial of service (stack exhaustion) in the dissect_IODWriteReq function in plugins/profinet/packet-dcerpc-pn-io.c.	wireshark	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4543
2778	CVE-2017-9763	MEDIUM	High	The grub_ext2_read_block function in fs/ext2.c in GNU GRUB before 2013-11-12, as used in shlr/grub/fs/ext2.c in radare2 1.5.0, allows remote attackers to cause a denial of service (excessive stack use and application crash) via a crafted binary file, related to use of a variable-size stack array.	grub	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4520
2779	CVE-2017-9756	Medium	High	The aarch64_ext_ldst_reglist function in opcodes/aarch64-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4513
2780	CVE-2017-9755	Medium	High	opcodes/i386-dis.c in GNU Binutils 2.28 does not consider the number of registers for bnd mode, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4487
2781	CVE-2017-9754	Medium	High	The process_otr function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, does not validate a certain offset, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4546
2782	CVE-2017-9753	Medium	High	The versados_mkobject function in bfd/versados.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, does not initialize a certain data structure, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4525
2783	CVE-2017-9752	Medium	High	bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file in the _bfd_vms_get_value and _bfd_vms_slurp_etir functions during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4571
2784	CVE-2017-9751	Medium	High	opcodes/rl78-decode.opc in GNU Binutils 2.28 has an unbounded GETBYTE macro, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4507
2785	CVE-2017-9750	Medium	High	opcodes/rx-decode.opc in GNU Binutils 2.28 lacks bounds checks for certain scale arrays, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4523
2786	CVE-2017-9749	Medium	High	The *regs* macros in opcodes/bfin-dis.c in GNU Binutils 2.28 allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4554
2787	CVE-2017-9748	Medium	High	The ieee_object_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, might allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution. NOTE: this may be related to a compiler bug.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4531
2788	CVE-2017-9747	Medium	High	The ieee_archive_p function in bfd/ieee.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, might allow remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution. NOTE: this may be related to a compiler bug.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4524
2789	CVE-2017-9746	Medium	High	The disassemble_bytes function in objdump.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of rae insns printing for this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4547
2790	CVE-2017-9745	Medium	High	The _bfd_vms_slurp_etir function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4519

	A	B	C	D	E	F	G	H	I	J	K	L	M
2791	CVE-2017-9744	Medium	High	The sh_elf_set_mach_from_flags function in bfd/elf32-sh.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4508
2792	CVE-2017-9743	Medium	High	The print_insn_score32 function in opcodes/score7-dis.c:552 in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4569
2793	CVE-2017-9742	Medium	High	The score_opcodes function in opcodes/score7-dis.c in GNU Binutils 2.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file, as demonstrated by mishandling of this file during objdump -D execution.	binutils	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4495
2794	CVE-2017-9740	MEDIUM	High	The xps_decode_font_char_imp function in xps/xpsfont.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4852
2795	CVE-2017-9739	MEDIUM	High	The Ins_JMPR function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	ghostscript	Unchanged	8.0.0.21	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4760
2796	CVE-2017-9731	MEDIUM	High	In meta/classes/package_ipk.bbclass in Poky in poky-pyro 17.0.0 for Yocto Project through YP Core - Pyro 2.3, attackers can obtain sensitive information by reading a URL in a Source entry in an ipk package.	yocto	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4545
2797	CVE-2017-9727	MEDIUM	High	The gx_ttfReader__Read function in base/gxttfb.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	ghostscript	Unchanged	8.0.0.21	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4812
2798	CVE-2017-9726	MEDIUM	High	The Ins_MDRP function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	ghostscript	Unchanged	8.0.0.21	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4759
2799	CVE-2017-9725	HIGH	High	In all Qualcomm products with Android releases from CAF using the Linux kernel, during DMA allocation, due to wrong data type of size, allocation size gets truncated which makes allocation succeed when it should fail.	linux	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1018-4337
2800	CVE-2017-9670	MEDIUM	High	An uninitialized stack variable vulnerability in load_tic_series() in set.c in gnuplot 5.2.rc1 allows an attacker to cause Denial of Service (Segmentation fault and Memory Corruption) or possibly have unspecified other impact when a victim opens a specially crafted file.	gnuplot	Unchanged	8.0.0.20	9.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4565
2801	CVE-2017-9620	MEDIUM	High	The xps_select_font_encoding function in xps/xpsfont.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document, related to the xps_encode_font_char_imp function.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4847
2802	CVE-2017-9619	MEDIUM	High	The xps_true_callback_glyph_name function in xps/xpsttf.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (Segmentation Violation and application crash) via a crafted file.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4767
2803	CVE-2017-9618	MEDIUM	High	The xps_load_sfnt_name function in xps/xpsfont.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted document.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4830
2804	CVE-2017-9617	Medium	High	In Wireshark 2.2.7, deeply nested DAAP data may cause stack exhaustion (uncontrolled recursion) in the dissect_daap_one_tag function in epan/dissectors/packet-daap.c in the DAAP dissector.	wireshark	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4528
2805	CVE-2017-9616	Medium	Medium	In Wireshark 2.2.7, overly deep mp4 chunks may cause stack exhaustion (uncontrolled recursion) in the dissect_mp4_box function in epan/dissectors/file-mp4.c.	wireshark	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4498
2806	CVE-2017-9614	MEDIUM	High	The fill_input_buffer function in jdatasrc.c in libjpeg-turbo 1.5.1 allows remote attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified other impact via a crafted jpg file.	libjpeg-turbo	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4766
2807	CVE-2017-9612	MEDIUM	High	The Ins_IP function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via a crafted document.	ghostscript	Unchanged	8.0.0.21	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4783
2808	CVE-2017-9611	MEDIUM	High	The Ins_MIRP function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	ghostscript	Unchanged	8.0.0.21	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4848
2809	CVE-2017-9610	MEDIUM	High	The xps_load_sfnt_name function in xps/xpsfont.c in Artifex Ghostscript GhostXPS 9.22 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4829
2810	CVE-2017-9608	MEDIUM	Medium	The dnxhd decoder in FFmpeg before 3.2.6, and 3.3.x before 3.3.3 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted mov file.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2945

	A	B	C	D	E	F	G	H	I	J	K	L	M
2811	CVE-2017-9605	MEDIUM	Medium	The vmw_gb_surface_define_ioctl function (accessible via DRM_IOCTL_VMW_GB_SURFACE_CREATE) in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.11.4 defines a backup_handle variable but does not give it an initial value. If one attempts to create a GB surface, with a previously allocated DMA buffer to be used as a backup buffer, the backup_handle variable does not get written to and is then later returned to user space, allowing local users to obtain sensitive information from uninitialized kernel memory via a crafted ioctl call.	linux	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4496
2812	CVE-2017-9545	MEDIUM	Medium	The next_text function in src/libmpg123/id3.c in mpg123 1.24.0 allows remote attackers to cause a denial of service (buffer over-read) via a crafted mp3 file.	mpg123	Unchanged	Won't Fix	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4790
2813	CVE-2017-9526	MEDIUM	Medium	In Libgcrypt before 1.7.7, an attacker who learns the EdDSA session key (from side-channel observation during the signing process) can easily recover the long-term secret key. 1.7.7 makes a cipher/ecc-eddsa.c change to store this session key in secure memory, to ensure that constant-time point operations are used in the MPI library.	libgcrypt	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4434
2814	CVE-2017-9524	MEDIUM	High	The qemu-nbd server in QEMU (aka Quick Emulator), when built with the Network Block Device (NBD) Server support, allows remote attackers to cause a denial of service (segmentation fault and server crash) by leveraging failure to ensure that all initialization occurs before talking to a client in the nbd_negotiate function.	qemu	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4637
2815	CVE-2017-9503	Low	Medium	QEMU (aka Quick Emulator), when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest OS privileged users to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors involving megasas command processing.	qemu	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4537
2816	CVE-2017-9502	MEDIUM	Medium	In curl before 7.54.1 on Windows and DOS, libcurl's default protocol function, which is the logic that allows an application to set which protocol libcurl should attempt to use when given a URL without a scheme part, had a flaw that could lead to it overwriting a heap based memory buffer with seven bytes. If the default protocol is specified to be FILE or a file: URL lacks two slashes, the given URL starts with a drive letter, and libcurl is built for Windows or DOS, then libcurl would copy the path 7 bytes off, so that the end of the given path would write beyond the malloc buffer (7 bytes being the length in bytes of the ascii string file://).	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4559
2817	CVE-2017-9501	MEDIUM	Medium	In ImageMagick 7.0.5-7 Q16, an assertion failure was found in the function LockSemaphoreInfo, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4380
2818	CVE-2017-9500	MEDIUM	Medium	In ImageMagick 7.0.5-8 Q16, an assertion failure was found in the function ResetImageProfileIterator, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4419
2819	CVE-2017-9499	MEDIUM	Medium	In ImageMagick 7.0.5-7 Q16, an assertion failure was found in the function SetPixelChannelAttributes, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4404
2820	CVE-2017-9469	MEDIUM	High	In Irssi before 1.0.3, when receiving certain incorrectly quoted DCC files, it tries to find the terminating quote one byte before the allocated memory. Thus, remote attackers might be able to cause a crash.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4411
2821	CVE-2017-9468	MEDIUM	High	In Irssi before 1.0.3, when receiving a DCC message without source nick/host, it attempts to dereference a NULL pointer. Thus, remote IRC servers can cause a crash.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4438
2822	CVE-2017-9462	HIGH	High	In Mercurial before 4.1.3, hg serve --stdio allows remote authenticated users to launch the Python debugger, and consequently execute arbitrary code, by using --debugger as a repository name.	mercurial	Unchanged	8.0.0.19	9.0.0.8	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-4396
2823	CVE-2017-9461	HIGH	High	smbd in Samba before 4.4.10 and 4.5.x before 4.5.6 has a denial of service vulnerability (fd_open_atomic infinite loop with high CPU usage and memory consumption) due to wrongly handling dangling symlinks.	samba	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4407
2824	CVE-2017-9445	MEDIUM	High	In systemd through 233, certain sizes passed to dns_packet_new in systemd-resolved can cause it to allocate a buffer that's too small. A malicious DNS server can exploit this via a response with a specially crafted TCP payload to trick systemd-resolved into allocating a buffer that's too small, and subsequently write arbitrary data beyond the end of it.	systemd	Unchanged	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4534
2825	CVE-2017-9440	MEDIUM	Medium	In ImageMagick 7.0.5-5, a memory leak was found in the function ReadPSDChannel in coders/psd.c, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4418
2826	CVE-2017-9439	MEDIUM	Medium	In ImageMagick 7.0.5-5, a memory leak was found in the function ReadPDBImage in coders/pdb.c, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4435
2827	CVE-2017-9412	MEDIUM	Medium	The unpack_read_samples function in frontend/get_audio.c in LAME 3.99.5 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted wav file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4792
2828	CVE-2017-9411	MEDIUM	Medium	The fill_buffer_resample function in libmp3lame/util.c in LAME 3.99.5 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted wav file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4800
2829	CVE-2017-9410	MEDIUM	Medium	The fill_buffer_resample function in libmp3lame/util.c in LAME 3.99.5 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted wav file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4862
2830	CVE-2017-9409	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadMPCImage function in mpc.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4403

	A	B	C	D	E	F	G	H	I	J	K	L	M
2831	CVE-2017-9408	MEDIUM	Medium	In Poppler 0.54.0, a memory leak vulnerability was found in the function Object::initArray in Object.cc, which allows attackers to cause a denial of service via a crafted file.	poppler	Unchanged	Won't Fix	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4384
2832	CVE-2017-9407	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadPALMImage function in palm.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4421
2833	CVE-2017-9406	MEDIUM	Medium	In Poppler 0.54.0, a memory leak vulnerability was found in the function gmalloc in gmem.cc, which allows attackers to cause a denial of service via a crafted file.	poppler	Unchanged	Won't Fix	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4399
2834	CVE-2017-9405	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadICONImage function in icon.c:452 allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4394
2835	CVE-2017-9404	MEDIUM	Medium	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function OJPEGReadHeaderInfoSecTablesQTable in tif_ojpeg.c, which allows attackers to cause a denial of service via a crafted file.	libtiff	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4379
2836	CVE-2017-9403	MEDIUM	Medium	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function TIFFReadDirEntryLong8Array in tif_dirread.c, which allows attackers to cause a denial of service via a crafted file.	libtiff	Unchanged	8.0.0.19	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4409
2837	CVE-2017-9375	Low	Medium	QEMU (aka Quick Emulator), when built with USB xHCI controller emulator support, allows local guest OS privileged users to cause a denial of service (infinite recursive call) via vectors involving control transfer descriptors sequencing.	qemu	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4503
2838	CVE-2017-9374	Low	Medium	Memory leak in QEMU (aka Quick Emulator), when built with USB EHCI Emulation support, allows local guest OS privileged users to cause a denial of service (memory consumption) by repeatedly hot-unplugging the device.	qemu	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4485
2839	CVE-2017-9373	Low	Medium	Memory leak in QEMU (aka Quick Emulator), when built with IDE AHCI Emulation support, allows local guest OS privileged users to cause a denial of service (memory consumption) by repeatedly hot-unplugging the AHCI device.	qemu	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4516
2840	CVE-2017-9354	MEDIUM	High	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the RGMP dissector could crash. This was addressed in epan/dissectors/packet-rgmp.c by validating an IPv4 address.	wireshark	Unchanged	8.0.0.22	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4417
2841	CVE-2017-9353	MEDIUM	High	In Wireshark 2.2.0 to 2.2.6, the IPv6 dissector could crash. This was addressed in epan/dissectors/packet-ipv6.c by validating an IPv6 address.	wireshark	Unchanged	8.0.0.22	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4428
2842	CVE-2017-9352	HIGH	High	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the Bazaar dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-bzr.c by ensuring that backwards parsing cannot occur.	wireshark	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4406
2843	CVE-2017-9351	MEDIUM	High	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DHCP dissector could read past the end of a buffer. This was addressed in epan/dissectors/packet-bootp.c by extracting the Vendor Class Identifier more carefully.	wireshark	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4392
2844	CVE-2017-9350	HIGH	High	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the openSAFETY dissector could crash or exhaust system memory. This was addressed in epan/dissectors/packet-opensafety.c by checking for a negative length.	wireshark	Unchanged	8.0.0.22	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4424
2845	CVE-2017-9349	HIGH	High	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DICOM dissector has an infinite loop. This was addressed in epan/dissectors/packet-dcm.c by validating a length value.	wireshark	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4377
2846	CVE-2017-9348	MEDIUM	High	In Wireshark 2.2.0 to 2.2.6, the DOF dissector could read past the end of a buffer. This was addressed in epan/dissectors/packet-dof.c by validating a size value.	wireshark	Unchanged	Not vulnerable	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4388
2847	CVE-2017-9347	MEDIUM	High	In Wireshark 2.2.0 to 2.2.6, the ROS dissector could crash with a NULL pointer dereference. This was addressed in epan/dissectors/asn1/ros/packet-ros-template.c by validating an OID.	wireshark	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4402
2848	CVE-2017-9346	HIGH	High	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the SoulSeek dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-slsk.c by making loop bounds more explicit.	wireshark	Unchanged	8.0.0.22	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4429
2849	CVE-2017-9345	HIGH	High	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the DNS dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-dns.c by trying to detect self-referencing pointers.	wireshark	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4383
2850	CVE-2017-9344	MEDIUM	High	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the Bluetooth L2CAP dissector could divide by zero. This was addressed in epan/dissectors/packet-btl2cap.c by validating an interval value.	wireshark	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4395
2851	CVE-2017-9343	MEDIUM	High	In Wireshark 2.2.0 to 2.2.6 and 2.0.0 to 2.0.12, the MSNIP dissector misuses a NULL pointer. This was addressed in epan/dissectors/packet-msnip.c by validating an IPv4 address.	wireshark	Unchanged	8.0.0.22	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4422
2852	CVE-2017-9330	LOW	Medium	QEMU (aka Quick Emulator), when built with the USB OHCI Emulation support, allows local guest OS users to cause a denial of service (infinite loop) by leveraging an incorrect return value.	qemu	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4431
2853	CVE-2017-9310	LOW	Medium	QEMU (aka Quick Emulator), when built with the e1000e NIC emulation support, allows local guest OS privileged users to cause a denial of service (infinite loop) via vectors related to setting the initial receive / transmit descriptor head (TDH/RDH) outside the allocated descriptor buffer.	qemu	Unchanged	Not vulnerable	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4410
2854	CVE-2017-9287	MEDIUM	Medium	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user with access to search the directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.	openldap	Unchanged	8.0.0.28	9.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4584
2855	CVE-2017-9265	HIGH	Critical	In Open vSwitch (OvS) v2.7.0, there is a buffer over-read while parsing the group mod OpenFlow message sent from the controller in `lib/ofp-util.c` in the function `ofputil_pull_ofp15_group_mod`.	openvswitch	Unchanged	8.0.0.28	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4398

	A	B	C	D	E	F	G	H	I	J	K	L	M
2856	CVE-2017-9264	HIGH	Critical	In lib/conntrack.c in the firewall implementation in Open vSwitch (OvS) 2.6.1, there is a buffer over-read while parsing malformed TCP, UDP, and IPv6 packets in the functions `extract_l3_ipv6`, `extract_l4_tcp`, and `extract_l4_udp` that can be triggered remotely.	openvswitch	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4390
2857	CVE-2017-9263	LOW	Medium	In Open vSwitch (OvS) 2.7.0, while parsing an OpenFlow role status message, there is a call to the abort() function for undefined role status reasons in the function `ofp_print_role_status_message` in `lib/ofp-print.c` that may be leveraged toward a remote DoS attack by a malicious switch.	openvswitch	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4433
2858	CVE-2017-9262	MEDIUM	Medium	In ImageMagick 7.0.5-6 Q16, the ReadJNGImage function in coders/png.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4426
2859	CVE-2017-9261	MEDIUM	Medium	In ImageMagick 7.0.5-6 Q16, the ReadMNGImage function in coders/png.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4387
2860	CVE-2017-9257	HIGH	Medium	The mp4ff_read_ctts function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4572
2861	CVE-2017-9256	HIGH	Medium	The mp4ff_read_stco function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4502
2862	CVE-2017-9255	HIGH	Medium	The mp4ff_read_stsc function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4509
2863	CVE-2017-9254	HIGH	Medium	The mp4ff_read_stts function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4530
2864	CVE-2017-9253	HIGH	Medium	The mp4ff_read_stsd function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4500
2865	CVE-2017-9242	MEDIUM	Medium	The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.	linux	Unchanged	8.0.0.20	9.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4423
2866	CVE-2017-9233	MEDIUM	High	XML External Entity vulnerability in libexpat 2.2.0 and earlier (Expat XML Parser Library) allows attackers to put the parser in an infinite loop using a malformed external entity definition from an external DTD.	expat	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4717
2867	CVE-2017-9229	MEDIUM	High	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A SIGSEGV occurs in left_adjust_char_head() during regular expression compilation. Invalid handling of reg->dmax in forward_search_range() could result in an invalid pointer dereference, normally as an immediate denial-of-service condition.	ruby & php	Unchanged	8.0.0.20	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4695
2868	CVE-2017-9228	HIGH	Critical	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write occurs in bitset_set_range() during regular expression compilation due to an uninitialized variable from an incorrect state transition. An incorrect state transition in parse_char_class() could create an execution path that leaves a critical local variable uninitialized until it's used as an index, resulting in an out-of-bounds write memory corruption.	ruby & php	Unchanged	8.0.0.20	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4694
2869	CVE-2017-9227	HIGH	Critical	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in mbc_enc_len() during regular expression searching. Invalid handling of reg->dmin in forward_search_range() could result in an invalid pointer dereference, as an out-of-bounds read from a stack buffer.	ruby & php	Unchanged	8.0.0.20	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4696
2870	CVE-2017-9226	HIGH	Critical	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write or read occurs in next_state_val() during regular expression compilation. Octal numbers larger than 0xff are not handled correctly in fetch_token() and fetch_token_in_cc(). A malformed regular expression containing an octal number in the form of '\700' would produce an invalid code point value larger than 0xff in next_state_val(), resulting in an out-of-bounds write memory corruption.	ruby & php	Unchanged	8.0.0.20	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4698
2871	CVE-2017-9224	HIGH	Critical	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in match_at() during regular expression searching. A logical error involving order of validation and access in match_at() could result in an out-of-bounds read from a stack buffer.	ruby & php	Unchanged	8.0.0.20	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4697
2872	CVE-2017-9223	MEDIUM	Medium	The mp4ff_read_stts function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4497

	A	B	C	D	E	F	G	H	I	J	K	L	M
2873	CVE-2017-9222	HIGH	Medium	The mp4ff_parse_tag function in common/mp4ff/mp4meta.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4555
2874	CVE-2017-9221	MEDIUM	Medium	The mp4ff_read_mdhd function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4505
2875	CVE-2017-9220	MEDIUM	Medium	The mp4ff_read_stco function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (memory allocation error) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4560
2876	CVE-2017-9219	MEDIUM	Medium	The mp4ff_read_stsc function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (memory allocation error and application crash) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4548
2877	CVE-2017-9218	MEDIUM	Medium	The mp4ff_read_stsd function in common/mp4ff/mp4atom.c in Freeware Advanced Audio Decoder 2 (FAAD2) 2.7 allows remote attackers to cause a denial of service (invalid memory read and application crash) via a crafted mp4 file.	faad2	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4536
2878	CVE-2017-9217	MEDIUM	High	systemd-resolved through 233 allows remote attackers to cause a denial of service (daemon crash) via a crafted DNS response with an empty question section.	systemd	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4415
2879	CVE-2017-9216	MEDIUM	Medium	libjbig2dec.a in Artifex jbig2dec 0.13, as used in MuPDF and Ghostscript, has a NULL pointer dereference in the jbig2_huffman_get function in jbig2_huffman.c. For example, the jbig2dec utility will crash (segmentation fault) when parsing an invalid file.	ghostscript	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4298
2880	CVE-2017-9214	HIGH	Critical	In Open vSwitch (OvS) 2.7.0, while parsing an OFPT_QUEUE_GET_CONFIG_REPLY type OFP 1.0 message, there is a buffer over-read that is caused by an unsigned integer underflow in the function `ofputil_pull_queue_get_config_reply10` in `lib/ofp-util.c`.	openvswitch	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4408
2881	CVE-2017-9211	MEDIUM	Medium	The crypto_skcipher_init_tfm function in crypto/skcipher.c in the Linux kernel through 4.11.2 relies on a setkey function that lacks a key-size check, which allows local users to cause a denial of service (NULL pointer dereference) via a crafted application.	linux	Unchanged	Not vulnerable	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4296
2882	CVE-2017-9150	LOW	Medium	The do_check function in kernel/bpf/verifier.c in the Linux kernel before 4.11.1 does not make the allow_ptr_leaks value available for restricting the output of the print_bpf_insn function, which allows local users to obtain sensitive address information via crafted bpf system calls.	linux	Unchanged	Not vulnerable	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4294
2883	CVE-2017-9148	HIGH	Critical	The TLS session cache in FreeRADIUS 2.1.1 through 2.1.7, 3.0.x before 3.0.14, 3.1.x before 2017-02-04, and 4.0.x before 2017-02-04 fails to reliably prevent resumption of an unauthenticated session, which allows remote attackers (such as malicious 802.1X supplicants) to bypass authentication via PEAP or TTLS.	freeradius	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4381
2884	CVE-2017-9147	MEDIUM	Medium	LibTIFF 4.0.7 has an invalid read in the _TIFFVGetField function in tif_dir.c, which might allow remote attackers to cause a denial of service (crash) via a crafted TIFF file.	libtiff	Unchanged	8.0.0.19	9.0.0.8	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-4277
2885	CVE-2017-9144	MEDIUM	Medium	In ImageMagick 7.0.5-5, a crafted RLE image can trigger a crash because of incorrect EOF handling in coders/rle.c.	imagemagick	Unchanged	8.0.0.19	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4301
2886	CVE-2017-9143	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadARTImage function in coders/art.c allows attackers to cause a denial of service (memory leak) via a crafted .art file.	imagemagick	Unchanged	8.0.0.19	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4312
2887	CVE-2017-9142	MEDIUM	Medium	In ImageMagick 7.0.5-7 Q16, a crafted file could trigger an assertion failure in the WriteBlob function in MagickCore/blob.c because of missing checks in the ReadOneJNGImage function in coders/png.c.	imagemagick	Unchanged	8.0.0.19	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4307
2888	CVE-2017-9141	MEDIUM	Medium	In ImageMagick 7.0.5-7 Q16, a crafted file could trigger an assertion failure in the ResetImageProfileIterator function in MagickCore/profile.c because of missing checks in the ReadDDSImage function in coders/dds.c.	imagemagick	Unchanged	8.0.0.19	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4304
2889	CVE-2017-9120	HIGH	CRITICAL	PHP 7.x through 7.1.5 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a long string because of an Integer overflow in mysqli_real_escape_string.	php	Unchanged	Not vulnerable	Not vulnerable	10.17.41.11	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4553
2890	CVE-2017-9119	HIGH	Critical	The i_zval_ptr_dtor function in Zend/zend_variables.h in PHP 7.1.5 allows attackers to cause a denial of service (memory consumption and application crash) or possibly have unspecified other impact by triggering crafted operations on array data structures.	php	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4311
2891	CVE-2017-9118	MEDIUM	HIGH	PHP 7.1.5 has an Out of bounds access in php_pcre_replace_impl via a crafted preg_replace call.	php	Unchanged	Not vulnerable	Not vulnerable	Vulnerable	Investigate	Not vulnerable	Not vulnerable	LIN10-4545
2892	CVE-2017-9117	HIGH	Critical	In LibTIFF 4.0.7, the program processes BMP images without verifying that biWidth and biHeight in the bitmap-information header match the actual input, leading to a heap-based buffer over-read in bmp2tiff.	libtiff	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4288
2893	CVE-2017-9098	MEDIUM	High	ImageMagick before 7.0.5-2 and GraphicsMagick before 1.3.24 use uninitialized memory in the RLE decoder, allowing an attacker to leak sensitive information from process memory space, as demonstrated by remote attacks against ImageMagick code in a long-running server process that converts image data on behalf of multiple users. This is caused by a missing initialization step in the ReadRLEImage function in coders/rle.c.	imagemagick	Unchanged	8.0.0.19	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4310

	A	B	C	D	E	F	G	H	I	J	K	L	M
2894	CVE-2017-9083	MEDIUM	Medium	poppler 0.54.0, as used in Evince and other products, has a NULL pointer dereference in the JPXStream::readUByte function in JPXStream.cc. For example, the perf_test utility will crash (segmentation fault) when parsing an invalid PDF file.	poppler	Unchanged	Won't Fix	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4292
2895	CVE-2017-9079	MEDIUM	Medium	Dropbear before 2017.75 might allow local users to read certain files as root, if the file has the authorized_keys file format with a command= option. This occurs because ~/.ssh/authorized_keys is read with root privileges and symlinks are followed.	dropbear	Unchanged	8.0.0.19	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4281
2896	CVE-2017-9078	HIGH	High	The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.	dropbear	Unchanged	8.0.0.19	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4279
2897	CVE-2017-9077	HIGH	High	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	linux	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4305
2898	CVE-2017-9076	HIGH	High	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	linux	Unchanged	8.0.0.19	9.0.0.8	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4285
2899	CVE-2017-9075	HIGH	High	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	linux	Unchanged	8.0.0.19	9.0.0.8	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4297
2900	CVE-2017-9074	HIGH	High	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.	linux	Unchanged	8.0.0.19	9.0.0.8	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4291
2901	CVE-2017-9060	MEDIUM	Medium	Memory leak in the virtio_gpu_set_scanout function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (memory consumption) via a large number of VIRTIO_GPU_CMD_SET_SCANOUT: commands.	qemu	Unchanged	Not vulnerable	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4405
2902	CVE-2017-9059	MEDIUM	Medium	The NFSv4 implementation in the Linux kernel through 4.11.1 allows local users to cause a denial of service (resource consumption) by leveraging improper channel callback shutdown when unmounting an NFSv4 filesystem, aka a module reference and kernel daemon leak.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4275
2903	CVE-2017-9051	HIGH	Critical	libav before 12.1 is vulnerable to an invalid read of size 1 due to NULL pointer dereferencing in the nsv_read_chunk function in libavformat/nsvdec.c.	libav	Unchanged	8.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4280
2904	CVE-2017-9050	MEDIUM	High	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictAddString function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for CVE-2016-1839.	libxml2	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4289
2905	CVE-2017-9049	MEDIUM	High	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictComputeFastKey function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for libxml2 Bug 759398.	libxml2	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4282
2906	CVE-2017-9048	MEDIUM	High	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a stack-based buffer overflow. The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. At the end of the routine, the function may strcat two more characters without checking whether the current strlen(buf) + 2 < size. This vulnerability causes programs that use libxml2, such as PHP, to crash.	libxml2	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4314
2907	CVE-2017-9047	MEDIUM	High	A buffer overflow was discovered in libxml2 20904-GITv2.9.4-16-g0741801. The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. The variable len is assigned strlen(buf). If the content->type is XML_ELEMENT_CONTENT_ELEMENT, then (i) the content->prefix is appended to buf (if it actually fits) whereupon (ii) content->name is written to the buffer. However, the check for whether the content->name actually fits also uses 'len' rather than the updated buffer length strlen(buf). This allows us to write about size many bytes beyond the allocated memory. This vulnerability causes programs that use libxml2, such as PHP, to crash.	libxml2	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4302
2908	CVE-2017-9044	MEDIUM	Medium	The print_symbol_for_build_attribute function in readelf.c in GNU Binutils 2017-04-12 allows remote attackers to cause a denial of service (invalid read and SEGV) via a crafted ELF file.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4286
2909	CVE-2017-9043	MEDIUM	High	readelf.c in GNU Binutils 2017-04-12 has a shift exponent too large for type unsigned long issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4300
2910	CVE-2017-9042	MEDIUM	High	readelf.c in GNU Binutils 2017-04-12 has a cannot be represented in type long issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4315

	A	B	C	D	E	F	G	H	I	J	K	L	M
2911	CVE-2017-9041	MEDIUM	Medium	GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to MIPS GOT mishandling in the process_mips_specific function in readelf.c.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4283
2912	CVE-2017-9040	MEDIUM	Medium	GNU Binutils 2017-04-03 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash), related to the process_mips_specific function in readelf.c, via a crafted ELF file that triggers a large memory-allocation attempt.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4308
2913	CVE-2017-9039	MEDIUM	Medium	GNU Binutils 2.28 allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file with many program headers, related to the get_program_headers function in readelf.c.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4306
2914	CVE-2017-9038	MEDIUM	Medium	GNU Binutils 2.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to the byte_get_little_endian function in elfcomm.c, the get_unwind_section_word function in readelf.c, and ARM unwind information that contains invalid word offsets.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4313
2915	CVE-2017-9023	MEDIUM	High	The ASN.1 parser in strongSwan before 5.5.3 improperly handles CHOICE types when the x509 plugin is enabled, which allows remote attackers to cause a denial of service (infinite loop) via a crafted certificate.	strongswan	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4341
2916	CVE-2017-9022	MEDIUM	High	The gmp plugin in strongSwan before 5.5.3 does not properly validate RSA public keys before calling mpz_powm_sec, which allows remote peers to cause a denial of service (floating point exception and process crash) via a crafted certificate.	strongswan	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4340
2917	CVE-2017-8925	LOW	Medium	The omninet_open function in drivers/usb/serial/omninet.c in the Linux kernel before 4.10.4 allows local users to cause a denial of service (tty exhaustion) by leveraging reference count mishandling.	linux	Unchanged	8.0.0.19	9.0.0.8	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4191
2918	CVE-2017-8924	LOW	Medium	The edge_bulk_in_callback function in drivers/usb/serial/io_ti.c in the Linux kernel before 4.10.4 allows local users to obtain sensitive information (in the dmesg ringbuffer and syslog) from uninitialized kernel memory by using a crafted USB device (posing as an io_ti USB serial device) to trigger an integer underflow.	linux	Unchanged	8.0.0.19	9.0.0.8	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4240
2919	CVE-2017-8923	HIGH	Critical	The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.	php	Unchanged	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4238
2920	CVE-2017-8890	HIGH	Critical	The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.	linux	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4218
2921	CVE-2017-8872	MEDIUM	Critical	The htmlParseTryOrFinish function in HTMLparser.c in libxml2 2.9.4 allows attackers to cause a denial of service (buffer over-read) or information disclosure.	libxml2	Unchanged	8.0.0.28	9.0.0.18	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-4183
2922	CVE-2017-8871	HIGH	Medium	The cr_parser_parse_selector_core function in cr-parser.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a crafted CSS file.	libcroco	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-4391
2923	CVE-2017-8855	MEDIUM	High	wolfSSL before 3.11.0 does not prevent wc_DhAgree from accepting a malformed DH key.	wolfssl	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4215
2924	CVE-2017-8854	MEDIUM	High	wolfSSL before 3.10.2 has an out-of-bounds memory access with loading crafted DH parameters, aka a buffer overflow triggered by a malformed temporary DH file.	wolfssl	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4212
2925	CVE-2017-8834	MEDIUM	Medium	The cr_tknzr_parse_comment function in cr-tknzr.c in libcroco 0.6.12 allows remote attackers to cause a denial of service (memory allocation error) via a crafted CSS file.	libcroco	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-4397
2926	CVE-2017-8831	HIGH	High	The saa7164_bus_get function in drivers/media/pci/saa7164/saa7164-bus.c in the Linux kernel through 4.10.14 allows local users to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact by changing a certain sequence-number value, aka a double fetch vulnerability.	linux	Unchanged	8.0.0.28	9.0.0.18	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4217
2927	CVE-2017-8830	MEDIUM	Medium	In ImageMagick 7.0.5-6, the ReadBMPImage function in bmp.c:1379 allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4194
2928	CVE-2017-8824	HIGH	High	The dccp_disconnect function in net/dccp/proto.c in the Linux kernel through 4.14.3 allows local users to gain privileges or cause a denial of service (use-after-free) via an AF_UNSPEC connect system call during the DCCP_LISTEN state.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2761
2929	CVE-2017-8818	HIGH	Critical	curl and libcurl before 7.57.0 on 32-bit platforms allow attackers to cause a denial of service (out-of-bounds access and application crash) or possibly have unspecified other impact because too little memory is allocated for interfacing to an SSL library.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2616
2930	CVE-2017-8817	HIGH	Critical	The FTP wildcard function in curl and libcurl before 7.57.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) or possibly have unspecified other impact via a string that ends with an '[' character.	curl	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2612
2931	CVE-2017-8816	HIGH	Critical	The NTLM authentication feature in curl and libcurl before 7.57.0 on 32-bit platforms allows attackers to cause a denial of service (integer overflow and resultant buffer overflow, and application crash) or possibly have unspecified other impact via vectors involving long user and password fields.	curl	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2634

	A	B	C	D	E	F	G	H	I	J	K	L	M
2932	CVE-2017-8804	HIGH	High	The xdr_bytes and xdr_string functions in the GNU C Library (aka glibc or libc6) 2.25 mishandle failures of buffer deserialization, which allows remote attackers to cause a denial of service (virtual memory allocation, or memory consumption if an overcommit setting is not used) via a crafted UDP packet to port 111, a related issue to CVE-2017-8779.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4226
2933	CVE-2017-8797	HIGH	High	The NFSv4 server in the Linux kernel before 4.11.3 does not properly validate the layout type when processing the NFSv4 pNFS GETDEVICEINFO or LAYOUTGET operand in a UDP packet from a remote attacker. This type value is uninitialized upon encountering certain error conditions. This value is used as an array index for dereferencing, which leads to an OOPS and eventually a DoS of knfsd and a soft-lockup of the whole system.	linux	Unchanged	8.0.0.20	9.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4660
2934	CVE-2017-8786	HIGH	Critical	pcre2test.c in PCRE2 10.23 allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4233
2935	CVE-2017-8779	HIGH	High	rpcbind through 0.2.4, LIBTIRPC through 1.0.1 and 1.0.2-rc through 1.0.2-rc3, and NTIRPC through 1.4.3 do not consider the maximum RPC data size during memory allocation for XDR strings, which allows remote attackers to cause a denial of service (memory consumption with no subsequent free) via a crafted UDP packet to port 111, aka rpcbomb.	rpcbind	Unchanged	8.0.0.21	9.0.0.9	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4207
2936	CVE-2017-8765	HIGH	Medium	The function named ReadICONImage in coders\icon.c in ImageMagick 7.0.5-5 has a memory leak vulnerability which can cause memory exhaustion via a crafted ICON file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4213
2937	CVE-2017-8421	HIGH	Medium	The function coff_set_alignment_hook in coffcode.h in Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a memory leak vulnerability which can cause memory exhaustion in objdump via a crafted PE file. Additional validation in dump_relocs_in_section in objdump.c can resolve this.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4192
2938	CVE-2017-8419	MEDIUM	High	LAME through 3.99.5 relies on the signed integer data type for values in a WAV or AIFF header, which allows remote attackers to cause a denial of service (stack-based buffer overflow or heap-based buffer overflow) or possibly have unspecified other impact via a crafted file, as demonstrated by mishandling of num_channels.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4221
2939	CVE-2017-8399	HIGH	Critical	PCRE2 before 2017-03-10 has an out-of-bounds write caused by a stack-based buffer overflow in pcre2_match.c, related to a pattern with very many captures.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4182
2940	CVE-2017-8398	MEDIUM	High	dwarf.c in GNU Binutils 2.28 is vulnerable to an invalid read of size 1 during dumping of debug information from a corrupt binary. This vulnerability causes programs that conduct an analysis of binary programs, such as objdump and readelf, to crash.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4222
2941	CVE-2017-8397	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read of size 1 and an invalid write of size 1 during processing of a corrupt binary containing reloc(s) with negative addresses. This vulnerability causes programs that conduct an analysis of binary programs using the libbfd library, such as objdump, to crash.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4187
2942	CVE-2017-8396	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read of size 1 because the existing reloc offset range tests didn't catch small negative offsets less than the size of the reloc field. This vulnerability causes programs that conduct an analysis of binary programs using the libbfd library, such as objdump, to crash.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4205
2943	CVE-2017-8395	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid write of size 8 because of missing a malloc() return-value check to see if memory had actually been allocated in the _bfd_generic_get_section_contents function. This vulnerability causes programs that conduct an analysis of binary programs using the libbfd library, such as objcopy, to crash.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4229
2944	CVE-2017-8394	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read of size 4 due to NULL pointer dereferencing of _bfd_elf_large_com_section. This vulnerability causes programs that conduct an analysis of binary programs using the libbfd library, such as objcopy, to crash.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4184
2945	CVE-2017-8393	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to a global buffer over-read error because of an assumption made by code that runs for objcopy and strip, that SHT_REL/SHR_RELA sections are always named starting with a .rel/.rela prefix. This vulnerability causes programs that conduct an analysis of binary programs using the libbfd library, such as objcopy and strip, to crash.	binutils	Unchanged	8.0.0.23	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4230
2946	CVE-2017-8392	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read of size 8 because of missing a check to determine whether symbols are NULL in the _bfd_dwarf2_find_nearest_line function. This vulnerability causes programs that conduct an analysis of binary programs using the libbfd library, such as objdump, to crash.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4186

	A	B	C	D	E	F	G	H	I	J	K	L	M
2947	CVE-2017-8386	MEDIUM	High	git-shell in git before 2.4.12, 2.5.x before 2.5.6, 2.6.x before 2.6.7, 2.7.x before 2.7.5, 2.8.x before 2.8.5, 2.9.x before 2.9.4, 2.10.x before 2.10.3, 2.11.x before 2.11.2, and 2.12.x before 2.12.3 might allow remote authenticated users to gain privileges via a repository name that starts with a - (dash) character.	git	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4401
2948	CVE-2017-8380	High	Critical	Buffer overflow in the megasas_mmio_write function in Qemu 2.9.0 allows remote attackers to have unspecified impact via unknown vectors.	qemu	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5288
2949	CVE-2017-8379	MEDIUM	Medium	Memory leak in the keyboard input event handlers support in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption) by rapidly generating large keyboard events.	qemu	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4309
2950	CVE-2017-8365	MEDIUM	Medium	The i2les_array function in pcm.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file.	libsndfile	Unchanged	8.0.0.19	9.0.0.8	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-4188
2951	CVE-2017-8363	MEDIUM	Medium	The flac_buffer_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted audio file.	libsndfile	Unchanged	8.0.0.19	9.0.0.8	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-4236
2952	CVE-2017-8362	MEDIUM	Medium	The flac_buffer_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (invalid read and application crash) via a crafted audio file.	libsndfile	Unchanged	8.0.0.19	9.0.0.8	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-4197
2953	CVE-2017-8361	MEDIUM	Medium	The flac_buffer_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted audio file.	libsndfile	Unchanged	8.0.0.19	9.0.0.8	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-4190
2954	CVE-2017-8357	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadEPTImage function in ept.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4200
2955	CVE-2017-8356	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadSUNImage function in sun.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4224
2956	CVE-2017-8355	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadMTVImage function in mtv.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4219
2957	CVE-2017-8354	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadBMPImage function in bmp.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4196
2958	CVE-2017-8353	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadPICTImage function in pict.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4209
2959	CVE-2017-8352	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadXWDImage function in xwd.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4231
2960	CVE-2017-8351	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadPCDImage function in pcd.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4216
2961	CVE-2017-8350	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadJNGImage function in png.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4198
2962	CVE-2017-8349	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadSFWImage function in sfw.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4227
2963	CVE-2017-8348	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadMATImage function in mat.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4210
2964	CVE-2017-8347	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadEXRImage function in exr.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4211
2965	CVE-2017-8346	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadDCMImage function in dcm.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4181
2966	CVE-2017-8345	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadMNGImage function in png.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4189
2967	CVE-2017-8344	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadPCXImage function in pcx.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4206
2968	CVE-2017-8343	MEDIUM	Medium	In ImageMagick 7.0.5-5, the ReadAAIImage function in aai.c allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4237
2969	CVE-2017-8309	HIGH	High	Memory leak in the audio/audio.c in QEMU (aka Quick Emulator) allows remote attackers to cause a denial of service (memory consumption) by repeatedly starting and stopping audio capture.	qemu	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4299
2970	CVE-2017-8287	HIGH	Critical	FreeType 2 before 2017-03-26 has an out-of-bounds write caused by a heap-based buffer overflow related to the t1_builder_close_contour function in psaux/psobjs.c.	freetype	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4193
2971	CVE-2017-8284	MEDIUM	HIGH	** DISPUTED ** The disas_insn function in target/i386/translate.c in QEMU before 2.9.0, when TCG mode without hardware acceleration is used, does not limit the instruction size, which allows local users to gain privileges by creating a modified basic block that injects code into a setuid program, as demonstrated by procmail. NOTE: the vendor has stated this bug does not violate any security guarantees QEMU makes.	qemu	Unchanged	8.0.0.32	9.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1019-3675
2972	CVE-2017-8283	HIGH	Critical	dpkg-source in dpkg 1.3.0 through 1.18.23 is able to use a non-GNU patch program and does not offer a protection mechanism for blank-indented diff hunks, which allows remote attackers to conduct directory traversal attacks via a crafted Debian source package, as demonstrated by use of dpkg-source on NetBSD.	dpkg	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4228

	A	B	C	D	E	F	G	H	I	J	K	L	M
2973	CVE-2017-8112	MEDIUM	Medium	hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (infinite loop and CPU consumption) via the message ring page count.	qemu	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4185
2974	CVE-2017-8106	MEDIUM	Medium	The handle_invept function in arch/x86/kvm/vmx.c in the Linux kernel 3.12 through 3.15 allows privileged KVM guest OS users to cause a denial of service (NULL pointer dereference and host OS crash) via a single-context INVEPT instruction with a NULL EPT pointer.	linux	Unchanged	8.0.0.18	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4130
2975	CVE-2017-8105	HIGH	Critical	FreeType 2 before 2017-03-24 has an out-of-bounds write caused by a heap-based buffer overflow related to the t1_decoder_parse_charstrings function in psaux/t1decode.c.	freetype	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4069
2976	CVE-2017-8086	MEDIUM	Medium	Memory leak in the v9fs_list_xattr function in hw/9pfs/9p-xattr.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (memory consumption) via vectors involving the orig_value variable.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4201
2977	CVE-2017-8072	HIGH	High	The cp2112_gpio_direction_input function in drivers/hid/hid-cp2112.c in the Linux kernel 4.9.x before 4.9.9 does not have the expected EIO error status for a zero-length report, which allows local users to have an unspecified impact via unknown vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4092
2978	CVE-2017-8071	LOW	Medium	drivers/hid/hid-cp2112.c in the Linux kernel 4.9.x before 4.9.9 uses a spinlock without considering that sleeping is possible in a USB HID request callback, which allows local users to cause a denial of service (deadlock) via unspecified vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4038
2979	CVE-2017-8070	HIGH	High	drivers/net/usb/catc.c in the Linux kernel 4.9.x before 4.9.11 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	8.0.0.18	9.0.0.7	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4044
2980	CVE-2017-8069	HIGH	High	drivers/net/usb/rtl8150.c in the Linux kernel 4.9.x before 4.9.11 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4047
2981	CVE-2017-8068	HIGH	High	drivers/net/usb/pegasus.c in the Linux kernel 4.9.x before 4.9.11 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4068
2982	CVE-2017-8067	HIGH	High	drivers/char/virtio_console.c in the Linux kernel 4.9.x and 4.10.x before 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4037
2983	CVE-2017-8066	HIGH	High	drivers/net/can/usb/gs_usb.c in the Linux kernel 4.9.x and 4.10.x before 4.10.2 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4122
2984	CVE-2017-8065	HIGH	High	crypto/ccm.c in the Linux kernel 4.9.x and 4.10.x through 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4012
2985	CVE-2017-8064	HIGH	High	drivers/media/usb/dvb-usb-v2/dvb_usb_core.c in the Linux kernel 4.9.x and 4.10.x before 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4042
2986	CVE-2017-8063	HIGH	High	drivers/media/usb/dvb-usb/cxusb.c in the Linux kernel 4.9.x and 4.10.x before 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4107
2987	CVE-2017-8062	HIGH	High	drivers/media/usb/dvb-usb/dw2102.c in the Linux kernel 4.9.x and 4.10.x before 4.10.4 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4049
2988	CVE-2017-8061	HIGH	High	drivers/media/usb/dvb-usb/dvb-usb-firmware.c in the Linux kernel 4.9.x and 4.10.x before 4.10.7 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4067

	A	B	C	D	E	F	G	H	I	J	K	L	M
2989	CVE-2017-7982	MEDIUM	Medium	Integer overflow in the plist_from_bin function in bplist.c in libimobiledevice/libplist before 2017-04-19 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted plist file.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4099
2990	CVE-2017-7980	MEDIUM	High	Heap-based buffer overflow in Cirrus CLGD 54xx VGA Emulator in Quick Emulator (Qemu) 2.8 and earlier allows local guest OS users to execute arbitrary code or cause a denial of service (crash) via vectors related to a VNC client updating its display after a VGA operation.	qemu	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4836
2991	CVE-2017-7979	HIGH	High	The cookie feature in the packet action API implementation in net/sched/act_api.c in the Linux kernel 4.11.x through 4.11-rc7 mishandles the tb nlattr array, which allows local users to cause a denial of service (uninitialized memory access and refcount underflow, and system hang or crash) or possibly have unspecified other impact via tc filter add commands in certain contexts. NOTE: this does not affect stable kernels, such as 4.10.x, from kernel.org.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4026
2992	CVE-2017-7975	MEDIUM	High	Artifex jbig2dec 0.13, as used in Ghostscript, allows out-of-bounds writes because of an integer overflow in the jbig2_build_huffman_table function in jbig2_huffman.c during operations on a crafted JBIG2 file, leading to a denial of service (application crash) or possibly execution of arbitrary code.	ghostscript	Unchanged	8.0.0.18	9.0.0.7	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4024
2993	CVE-2017-7961	MEDIUM	HIGH	** DISPUTED ** The cr_tknzr_parse_rgb function in cr-tknzr.c in libcroco 0.6.11 and 0.6.12 has an outside the range of representable values of type long undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted CSS file. NOTE: third-party analysis reports This is not a security issue in my view. The conversion surely is truncating the double into a long value, but there is no impact as the value is one of the RGB components.	libcroco	Unchanged	8.0.0.32	9.0.0.25	10.17.41.19	10.18.44.14	Not vulnerable	Investigate	LIN1019-3677
2994	CVE-2017-7960	MEDIUM	Medium	The cr_input_new_from_uri function in cr-input.c in libcroco 0.6.11 and 0.6.12 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted CSS file.	libcroco	Unchanged	8.0.0.18	9.0.0.7	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-4145
2995	CVE-2017-7948	MEDIUM	High	Integer overflow in the mark_curve function in Artifex Ghostscript 9.21 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via a crafted PostScript document.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4133
2996	CVE-2017-7943	MEDIUM	Medium	The ReadSVGImage function in svg.c in ImageMagick 7.0.5-4 allows remote attackers to consume an amount of available memory via a crafted file.	imagemagick	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4117
2997	CVE-2017-7942	MEDIUM	Medium	The ReadAVSImage function in avs.c in ImageMagick 7.0.5-4 allows remote attackers to consume an amount of available memory via a crafted file.	imagemagick	Unchanged	8.0.0.28	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4078
2998	CVE-2017-7941	MEDIUM	Medium	The ReadSGIImage function in sgi.c in ImageMagick 7.0.5-4 allows remote attackers to consume an amount of available memory via a crafted file.	imagemagick	Unchanged	8.0.0.28	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4131
2999	CVE-2017-7895	HIGH	Critical	The NFSv2 and NFSv3 server implementations in the Linux kernel through 4.10.13 lack certain checks for the end of a buffer, which allows remote attackers to trigger pointer-arithmetic errors or possibly have unspecified other impact via crafted requests, related to fs/nfsd/nfs3xdr.c and fs/nfsd/nfsxdr.c.	linux	Unchanged	8.0.0.18	9.0.0.7	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4204
3000	CVE-2017-7890	MEDIUM	Medium	The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read −700 bytes from the top of the stack, potentially disclosing sensitive information.	php	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5048
3001	CVE-2017-7889	HIGH	High	The mm subsystem in the Linux kernel through 4.10.10 does not properly enforce the CONFIG_STRICT_DEVMEM protection mechanism, which allows local users to read or write to kernel memory locations in the first megabyte (and bypass slab-allocation access restrictions) via an application that opens the /dev/mem file, related to arch/x86/mm/init.c and drivers/char/mem.c.	linux	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4076
3002	CVE-2017-7869	MEDIUM	High	GnuTLS before 2017-02-20 has an out-of-bounds write caused by an integer overflow and heap-based buffer overflow related to the cdk_pkt_read function in opencdk/read-packet.c. This issue (which is a subset of the vendor's GNUTLS-SA-2017-3 report) is fixed in 3.5.10.	gnutls	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4034
3003	CVE-2017-7868	MEDIUM	High	International Components for Unicode (ICU) for C/C++ before 2017-02-13 has an out-of-bounds write caused by a heap-based buffer overflow related to the utf8TextAccess function in common/utext.cpp and the utext_moveIndex32* function.	icu	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4061
3004	CVE-2017-7867	MEDIUM	High	International Components for Unicode (ICU) for C/C++ before 2017-02-13 has an out-of-bounds write caused by a heap-based buffer overflow related to the utf8TextAccess function in common/utext.cpp and the utext_setNativeIndex* function.	icu	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4119
3005	CVE-2017-7866	HIGH	Critical	FFmpeg before 2017-01-23 has an out-of-bounds write caused by a stack-based buffer overflow related to the decode_zbuf function in libavcodec/pngdec.c.	ffmpeg	Unchanged	Won't Fix	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4079
3006	CVE-2017-7865	HIGH	Critical	FFmpeg before 2017-01-24 has an out-of-bounds write caused by a heap-based buffer overflow related to the ipvideo_decode_block_opcode_0xA function in libavcodec/interplayvideo.c and the avcodec_align_dimensions2 function in libavcodec/utils.c.	ffmpeg	Unchanged	Won't Fix	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4141
3007	CVE-2017-7864	HIGH	Critical	FreeType 2 before 2017-02-02 has an out-of-bounds write caused by a heap-based buffer overflow related to the tt_size_reset function in truetype/ttobjs.c.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4096

	A	B	C	D	E	F	G	H	I	J	K	L	M
3008	CVE-2017-7863	HIGH	Critical	FFmpeg before 2017-02-04 has an out-of-bounds write caused by a heap-based buffer overflow related to the decode_frame_common function in libavcodec/pngdec.c.	ffmpeg	Unchanged	Won't Fix	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4127
3009	CVE-2017-7862	HIGH	Critical	FFmpeg before 2017-02-07 has an out-of-bounds write caused by a heap-based buffer overflow related to the decode_frame function in libavcodec/pictordec.c.	ffmpeg	Unchanged	Won't Fix	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4020
3010	CVE-2017-7859	HIGH	Critical	FFmpeg before 2017-03-05 has an out-of-bounds write caused by a heap-based buffer overflow related to the ff_h264_slice_context_init function in libavcodec/h264dec.c.	ffmpeg	Unchanged	Won't Fix	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4118
3011	CVE-2017-7858	HIGH	Critical	FreeType 2 before 2017-03-07 has an out-of-bounds write related to the TT_Get_MM_Var function in truetype/ttgxvar.c and the sfnt_init_face function in sfnt/sfobjs.c.	freetype	Unchanged	Not vulnerable	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4109
3012	CVE-2017-7857	HIGH	Critical	FreeType 2 before 2017-03-08 has an out-of-bounds write caused by a heap-based buffer overflow related to the TT_Get_MM_Var function in truetype/ttgxvar.c and the sfnt_init_face function in sfnt/sfobjs.c.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4115
3013	CVE-2017-7748	HIGH	High	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the WSP dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-wsp.c by adding a length check.	wireshark	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4139
3014	CVE-2017-7747	MEDIUM	High	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the PacketBB dissector could crash, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-packetbb.c by restricting additions to the protocol tree.	wireshark	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4015
3015	CVE-2017-7746	HIGH	High	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the SLSK dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-slsk.c by adding checks for the remaining length.	wireshark	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4055
3016	CVE-2017-7745	HIGH	High	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the SIGCOMP dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-sigcomp.c by correcting a memory-size check.	wireshark	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4063
3017	CVE-2017-7742	MEDIUM	Medium	In libsndfile before 1.0.28, an error in the flac_buffer_copy() function (flac.c) can be exploited to cause a segmentation violation (with read memory access) via a specially crafted FLAC file during a resample attempt, a similar issue to CVE-2017-7585.	libsndfile	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4128
3018	CVE-2017-7741	MEDIUM	Medium	In libsndfile before 1.0.28, an error in the flac_buffer_copy() function (flac.c) can be exploited to cause a segmentation violation (with write memory access) via a specially crafted FLAC file during a resample attempt, a similar issue to CVE-2017-7585.	libsndfile	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4066
3019	CVE-2017-7718	LOW	Medium	hw/display/cirrus_vga_rop.h in QEMU (aka Quick Emulator) allow local guest OS privileged users to cause a denial of service (out-of-bounds read and QEMU process crash) via vectors related to copying VGA data via the cirrus_bitblt_rop_fwd_transp_ and cirrus_bitblt_rop_fwd_ functions.	qemu	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4033
3020	CVE-2017-7705	HIGH	High	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the RPC over RDMA dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-rpcrdma.c by correctly checking for going beyond the maximum offset.	wireshark	Unchanged	Not vulnerable	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4046
3021	CVE-2017-7704	HIGH	High	In Wireshark 2.2.0 to 2.2.5, the DOF dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-dof.c by using a different integer data type and adjusting a return value.	wireshark	Unchanged	Not vulnerable	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4048
3022	CVE-2017-7703	MEDIUM	High	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the IMAP dissector could crash, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-imap.c by calculating a line's end correctly.	wireshark	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4105
3023	CVE-2017-7702	HIGH	High	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the WBXML dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-wbxml.c by adding length validation.	wireshark	Unchanged	8.0.0.28	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4100
3024	CVE-2017-7701	HIGH	High	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the BGP dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-bgp.c by using a different integer data type.	wireshark	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4124
3025	CVE-2017-7700	HIGH	Medium	In Wireshark 2.2.0 to 2.2.5 and 2.0.0 to 2.0.11, the NetScaler file parser could go into an infinite loop, triggered by a malformed capture file. This was addressed in wiretap/netscaler.c by ensuring a nonzero record size.	wireshark	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4050
3026	CVE-2017-7679	HIGH	Critical	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	apache2	Unchanged	8.0.0.20	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4557
3027	CVE-2017-7668	HIGH	Critical	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.	apache2	Unchanged	8.0.0.20	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4486
3028	CVE-2017-7659	MEDIUM	High	A maliciously constructed HTTP/2 request could cause mod_http2 2.4.24, 2.4.25 to dereference a NULL pointer and crash the server process.	apache2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4823
3029	CVE-2017-7655	Medium	HIGH	In Eclipse Mosquitto version from 1.0 to 1.4.15, a Null Dereference vulnerability was found in the Mosquitto library which could lead to crashes for those applications using the library.	mosquitto	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3813

	A	B	C	D	E	F	G	H	I	J	K	L	M
3030	CVE-2017-7654	MEDIUM	HIGH	In Eclipse Mosquitto 1.4.15 and earlier, a Memory Leak vulnerability was found within the Mosquitto Broker. Unauthenticated clients can send crafted CONNECT packets which could cause a denial of service in the Mosquitto Broker.	mosquitto	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4125
3031	CVE-2017-7653	LOW	MEDIUM	The Eclipse Mosquitto broker up to version 1.4.15 does not reject strings that are not valid UTF-8. A malicious client could cause other clients that do reject invalid UTF-8 strings to disconnect themselves from the broker by sending a topic string which is not valid UTF-8, and so cause a denial of service for the clients.	mosquitto	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4110
3032	CVE-2017-7645	HIGH	High	The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers to cause a denial of service (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c.	linux	Unchanged	8.0.0.19	9.0.0.8	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4123
3033	CVE-2017-7619	MEDIUM	High	In ImageMagick 7.0.4-9, an infinite loop can occur because of a floating-point rounding error in some of the color algorithms. This affects ModulateHSL, ModulateHCL, ModulateHCLp, ModulateHSB, ModulateHSI, ModulateHSV, ModulateHWB, ModulateLCHab, and ModulateLCHuv.	imagemagick	Unchanged	8.0.0.28	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3960
3034	CVE-2017-7618	HIGH	High	crypto/ahash.c in the Linux kernel through 4.10.9 allows attackers to cause a denial of service (API operation calling its own callback, and infinite recursion) by triggering EBUSY on a full queue.	linux	Unchanged	8.0.0.17	9.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3971
3035	CVE-2017-7616	LOW	Medium	Incorrect error handling in the set_mempolicy and mbind compat syscalls in mm/mempolicy.c in the Linux kernel through 4.10.9 allows local users to obtain sensitive information from uninitialized stack data by triggering failure of a certain bitmap operation.	linux	Unchanged	8.0.0.17	9.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3957
3036	CVE-2017-7614	HIGH	Critical	elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a member access within null pointer undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an int main() {return 0;} program.	binutils	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3945
3037	CVE-2017-7613	MEDIUM	Medium	elflint.c in elfutils 0.168 does not validate the number of sections and the number of segments, which allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.	elfutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3965
3038	CVE-2017-7612	MEDIUM	Medium	The check_sysv_hash function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.	elfutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3892
3039	CVE-2017-7611	MEDIUM	Medium	The check_symtab_shndx function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.	elfutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3922
3040	CVE-2017-7610	MEDIUM	Medium	The check_group function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.	elfutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3931
3041	CVE-2017-7609	MEDIUM	Medium	elf_compress.c in elfutils 0.168 does not validate the zlib compression factor, which allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.	elfutils	Unchanged	Not vulnerable	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3954
3042	CVE-2017-7608	MEDIUM	Medium	The ebl_object_note_type_name function in eblobjnotetypename.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.	elfutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3926
3043	CVE-2017-7607	MEDIUM	Medium	The handle_gnu_hash function in readelf.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.	elfutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3939
3044	CVE-2017-7606	MEDIUM	Medium	coders/rle.c in ImageMagick 7.0.5-4 has an outside the range of representable values of type unsigned char undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.	imagemagick	Unchanged	8.0.0.28	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3893
3045	CVE-2017-7602	MEDIUM	High	LibTIFF 4.0.7 has a signed integer overflow, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3880
3046	CVE-2017-7601	MEDIUM	High	LibTIFF 4.0.7 has a shift exponent too large for 64-bit type long undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3909
3047	CVE-2017-7600	MEDIUM	High	LibTIFF 4.0.7 has an outside the range of representable values of type unsigned char undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3891
3048	CVE-2017-7599	MEDIUM	High	LibTIFF 4.0.7 has an outside the range of representable values of type short undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3936
3049	CVE-2017-7598	MEDIUM	High	tif_dirread.c in LibTIFF 4.0.7 might allow remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3949
3050	CVE-2017-7597	MEDIUM	High	tif_dirread.c in LibTIFF 4.0.7 has an outside the range of representable values of type float undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3963

	A	B	C	D	E	F	G	H	I	J	K	L	M
3051	CVE-2017-7596	MEDIUM	High	LibTIFF 4.0.7 has an outside the range of representable values of type float undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3918
3052	CVE-2017-7595	MEDIUM	Medium	The JPEGSetupEncode function in tiff_jpeg.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3890
3053	CVE-2017-7594	MEDIUM	Medium	The OJPEGReadHeaderInfoSecTablesDcTable function in tif_ojpeg.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (memory leak) via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3914
3054	CVE-2017-7593	MEDIUM	Medium	tif_read.c in LibTIFF 4.0.7 does not ensure that tif_rawdata is properly initialized, which might allow remote attackers to obtain sensitive information from process memory via a crafted image.	tiff	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3972
3055	CVE-2017-7592	MEDIUM	High	The putagreytile function in tif_getimage.c in LibTIFF 4.0.7 has a left-shift undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3964
3056	CVE-2017-7586	MEDIUM	Medium	In libsndfile before 1.0.28, an error in the header_read() function (common.c) when handling ID3 tags can be exploited to cause a stack-based buffer overflow via a specially crafted FLAC file.	libsndfile	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3968
3057	CVE-2017-7585	MEDIUM	Medium	In libsndfile before 1.0.28, an error in the flac_buffer_copy() function (flac.c) can be exploited to cause a stack-based buffer overflow via a specially crafted FLAC file.	libsndfile	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3934
3058	CVE-2017-7562	MEDIUM	MEDIUM	A flaw was found in krb5 certificate EKU validation which could lead to improper authorization if a forged certificate with the right EKU and no SAN is used.	krb5	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4278
3059	CVE-2017-7558	MEDIUM	HIGH	A kernel data leak due to an out-of-bound read was found in Linux kernel in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info() functions present since v4.7-rc1 upto v4.13 including. A data leak happens when these functions fill in sockaddr data structures used to export socket's diagnostic information. As a result upto 100 bytes of the slab data could be leaked to a userspace.	linux	Unchanged	Not vulnerable	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4174
3060	CVE-2017-7548	MEDIUM	High	PostgreSQL versions before 9.4.13, 9.5.8 and 9.6.4 are vulnerable to authorization flaw allowing remote authenticated attackers with no privileges on a large object to overwrite the entire contents of the object, resulting in a denial of service.	postgresql	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5154
3061	CVE-2017-7547	MEDIUM	High	PostgreSQL versions before 9.2.22, 9.3.18, 9.4.13, 9.5.8 and 9.6.4 are vulnerable to authorization flaw allowing remote authenticated attackers to retrieve passwords from the user mappings defined by the foreign server owners without actually having the privileges to do so.	postgresql	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5133
3062	CVE-2017-7546	High	Critical	PostgreSQL versions before 9.2.22, 9.3.18, 9.4.13, 9.5.8 and 9.6.4 are vulnerable to incorrect authentication flaw allowing remote attackers to gain access to database accounts with an empty password.	postgresql	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5119
3063	CVE-2017-7544	MEDIUM	Critical	libexif through 0.6.21 is vulnerable to out-of-bounds heap read vulnerability in exif_data_save_data_entry function in libexif/exif-data.c caused by improper length computation of the allocated data of an ExifMnote entry which can cause denial-of-service or possibly information disclosure.	libexif	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5436
3064	CVE-2017-7542	MEDIUM	Medium	The ip6_find_1stfragopt function in net/ipv6/output_core.c in the Linux kernel through 4.12.3 allows local users to cause a denial of service (integer overflow and infinite loop) by leveraging the ability to open a raw socket.	linux	Unchanged	8.0.0.21	9.0.0.10	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4822
3065	CVE-2017-7541	HIGH	High	The brcmf_cfg80211_mgmt_tx function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.12.3 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted NL80211_CMD_FRAME Netlink packet.	linux	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4768
3066	CVE-2017-7539	MEDIUM	HIGH	Quick Emulator(Qemu) built with the Network Block Device(NBD) Server support is vulnerable to a crash via assertion failure. It could occur if a client sent undue data during initial connection negotiation.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4281
3067	CVE-2017-7533	Medium	High	Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_handle_event and vfs_rename functions.	linux	Unchanged	8.0.0.21	9.0.0.10	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5065
3068	CVE-2017-7529	MEDIUM	High	Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.	nginx	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4757
3069	CVE-2017-7526	MEDIUM	MEDIUM	Libgcrypt's RSA-1024 implementation using left-to-right method for computing the sliding-window expansion was found to be vulnerable to cache side-channel attack resulting into complete break of RSA-1024. The same attack is believed to work on RSA-2048 with moderately more computation. This side-channel requires that attacker can run arbitrary software on the hardware where the private RSA key is used.	libgcrypt	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4733
3070	CVE-2017-7522	MEDIUM	Medium	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to denial-of-service by authenticated remote attacker via sending a certificate with an embedded NULL character.	openvpn	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4504
3071	CVE-2017-7521	MEDIUM	Medium	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to remote denial-of-service due to memory exhaustion caused by memory leaks and double-free issue in extract_x509_extension().	openvpn	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4550

	A	B	C	D	E	F	G	H	I	J	K	L	M
3072	CVE-2017-7520	MEDIUM	High	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to denial-of-service and/or possibly sensitive memory leak triggered by man-in-the-middle attacker.	openvpn	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4549
3073	CVE-2017-7519	LOW	MEDIUM	In Ceph, a format string flaw was found in the way libradosstriper parses input from user. A user could crash an application or service using the libradosstriper library.	ceph	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4392
3074	CVE-2017-7518	MEDIUM	HIGH	Linux kernel built with the Kernel-based Virtual Machine(CONFIG_KVM) support is vulnerable to an incorrect debug exception(#DB) error. It could occur while emulating a syscall instruction. A user/process inside guest could use this flaw to potentially escalate their privileges inside guest.	linux	Unchanged	8.0.0.27	9.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4172
3075	CVE-2017-7516			It was found that the cpio --no-absolute-filenames option since version 2.7 did not verify paths during extraction. A specially crafted cpio archive could bypass this option and write to an arbitrary location, outside of the extraction directory.	cpio	Updated	8.0.0.30	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3232
3076	CVE-2017-7515	MEDIUM	Medium	poppler through version 0.55.0 is vulnerable to an uncontrolled recursion in pdfunite resulting into potential denial-of-service.	poppler	Unchanged	Won't Fix	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4432
3077	CVE-2017-7511	MEDIUM	Medium	poppler since version 0.17.3 has been vulnerable to NULL pointer dereference in pdfunite triggered by specially crafted documents.	poppler	Unchanged	Won't Fix	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4427
3078	CVE-2017-7510	Medium	HIGH	In ovirt-engine 4.1, if a host was provisioned with cloud-init, the root password could be revealed through the REST interface.	ovirt-engine	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	New
3079	CVE-2017-7508	MEDIUM	High	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to remote denial-of-service when receiving malformed IPv6 packet.	openvpn	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4522
3080	CVE-2017-7507	MEDIUM	High	GnuTLS version 3.5.12 and earlier is vulnerable to a NULL pointer dereference while decoding a status response TLS extension with valid contents. This could lead to a crash of the GnuTLS server application.	gnutls	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4489
3081	CVE-2017-7506	MEDIUM	High	spice versions though 0.13 are vulnerable to out-of-bounds memory access when processing specially crafted messages from authenticated attacker to the spice server resulting into crash and/or server memory leak.	spice	Unchanged	8.0.0.30	9.0.0.21	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4799
3082	CVE-2017-7502	MEDIUM	High	Null pointer dereference vulnerability in NSS since 3.24.0 was found when server receives empty SSLv2 messages resulting into denial of service by remote attacker.	nss	Unchanged	Not vulnerable	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4389
3083	CVE-2017-7501	MEDIUM	High	It was found that versions of rpm before 4.13.0.2 use temporary files with predictable names when installing an RPM. An attacker with ability to write in a directory where files will be installed could create symbolic links to an arbitrary location and modify content, and possibly permissions to arbitrary files, which could be used for denial of service or possibly privilege escalation.	rpm	Unchanged	Vulnerable	Not vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2619
3084	CVE-2017-7495	LOW	Medium	fs/ext4/inode.c in the Linux kernel before 4.6.2, when ext4 data=ordered mode is used, mishandles a needs-flushing-before-commit list, which allows local users to obtain sensitive information from other users' files in opportunistic circumstances by waiting for a hardware reset, creating a new file, making write system calls, and reading this file.	linux	Unchanged	8.0.0.20	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4276
3085	CVE-2017-7494	HIGH	Critical	Samba since version 3.5.0 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.	samba	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4416
3086	CVE-2017-7493	MEDIUM	High	Quick Emulator (Qemu) built with the VirtFS, host directory sharing via Plan 9 File System(9pfs) support, is vulnerable to an improper access control issue. It could occur while accessing virtfs metadata files in mapped-file security mode. A guest user could use this flaw to escalate their privileges inside guest.	qemu	Unchanged	8.0.0.27	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4214
3087	CVE-2017-7487	HIGH	High	The ipxitf_ioctl function in net/ipx/af_ipx.c in the Linux kernel through 4.11.1 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a failed SIOCGIFADDR ioctl call for an IPX interface.	linux	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4284
3088	CVE-2017-7486	MEDIUM	High	PostgreSQL versions 8.4 - 9.6 are vulnerable to information leak in pg_user_mappings view which discloses foreign server passwords to any user having USAGE privilege on the associated foreign server.	postgresql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4202
3089	CVE-2017-7485	MEDIUM	Medium	In PostgreSQL 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3, it was found that the PGREQUIRESSL environment variable was no longer enforcing a SSL/TLS connection to a PostgreSQL server. An active Man-in-the-Middle attacker could use this flaw to strip the SSL/TLS protection from a connection between a client and a server.	postgresql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4208
3090	CVE-2017-7484	MEDIUM	High	It was found that some selectivity estimation functions in PostgreSQL before 9.2.21, 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3 did not check user privileges before providing information from pg_statistic, possibly leaking information. An unprivileged attacker could use this flaw to steal some information from tables they are otherwise not allowed to access.	postgresql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4223

	A	B	C	D	E	F	G	H	I	J	K	L	M
3091	CVE-2017-7482	HIGH	HIGH	When a kerberos 5 ticket is being decoded so that it can be loaded into an rxrpc-type key, the length of a variable-length field is checked to make sure that it's not going to overrun the allocated buffer space. The data is padded to the nearest four-byte boundary and the code doesn't check for this extra four-byte aligned padding. This can lead to the size-remaining variable wrapping and the data pointer accessing or reading past the end of the buffer. The read functionality could allow for a 3 byte infoleak and the write flaw could allow for an uncontrolled 3 byte write to kernels slab memory. This could lead to memory corruption and possible privilege escalation although no known exploit exists at the time of writing.	linux	Unchanged	8.0.0.27	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4178
3092	CVE-2017-7479	MEDIUM	Medium	OpenVPN versions before 2.3.15 and before 2.4.2 are vulnerable to reachable assertion when packet-ID counter rolls over resulting into Denial of Service of server by authenticated attacker.	openvpn	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4303
3093	CVE-2017-7478	MEDIUM	High	OpenVPN version 2.3.12 and newer is vulnerable to unauthenticated Denial of Service of server via received large control packet. Note that this issue is fixed in 2.3.15 and 2.4.2.	openvpn	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4274
3094	CVE-2017-7477	MEDIUM	High	Heap-based buffer overflow in drivers/net/macsec.c in the MACsec module in the Linux kernel through 4.10.12 allows attackers to cause a denial of service or possibly have unspecified other impact by leveraging the use of a MAX_SKB_FRAGS+1 size in conjunction with the NETIF_F_FRAGLIST feature, leading to an error in the skb_to_sgvec function.	linux	Unchanged	Not vulnerable	9.0.0.7	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4214
3095	CVE-2017-7476	HIGH	Critical	Gnulib before 2017-04-26 has a heap-based buffer overflow with the TZ environment variable. The error is in the save_abbr function in time_rz.c.	gnulib	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4203
3096	CVE-2017-7475	MEDIUM	Medium	Cairo version 1.15.4 is vulnerable to a NULL pointer dereference related to the FT_Load_Glyph and FT_Render_Glyph resulting in an application crash.	cairo	Unchanged	8.0.0.30	9.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4293
3097	CVE-2017-7472	MEDIUM	Medium	The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (memory consumption) via a series of KEY_REQKEY_DEFL_THREAD_KEYRING keyctl_set_reqkey_keyring calls.	linux	Unchanged	8.0.0.18	9.0.0.7	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4225
3098	CVE-2017-7471	HIGH	CRITICAL	Quick Emulator(Qemu) built with the VirtFS, host directory sharing via Plan 9 File System(9pfs) support, is vulnerable to an improper access control issue. It could occur while accessing files on a shared host directory.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4202
3099	CVE-2017-7468	MEDIUM	HIGH	libcurl would attempt to resume a TLS session even if the client certificate had changed. That is unacceptable since a server by specification is allowed to skip the client certificate check on resume, and may instead use the old identity which was established by the previous certificate (or no certificate). unexpectedly with an assertion failure via a specially crafted command.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4035
3100	CVE-2017-7467	HIGH	CRITICAL	A buffer overflow flaw was found in the way minicom before version 2.7.1 handled VT100 escape sequences. A malicious terminal device could potentially use this flaw to crash minicom, or execute arbitrary code in the context of the minicom process.	minicom	Unchanged	8.0.0.27	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4306
3101	CVE-2017-7418	LOW	Medium	ProFTPD before 1.3.5e and 1.3.6 before 1.3.6rc5 controls whether the home directory of a user could contain a symbolic link through the AllowChrootSymlinks configuration option, but checks only the last path component when enforcing AllowChrootSymlinks. Attackers with local access could bypass the AllowChrootSymlinks control by replacing a path component (other than the last one) with a symbolic link. The threat model includes an attacker who is not granted full filesystem access by a hosting provider, but can reconfigure the home directory of an FTP user.	proftpd	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3879
3102	CVE-2017-7407	LOW	Low	The ourWriteOut function in tool_writeout.c in curl 7.53.1 might allow physically proximate attackers to obtain sensitive information from process memory in opportunistic circumstances by reading a workstation screen during use of a --write-out argument ending in a '%' character, which leads to a heap-based buffer over-read.	curl	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3902
3103	CVE-2017-7401	MEDIUM	High	Incorrect interaction of the parse_packet() and parse_part_sign_sha256() functions in network.c in collectd 5.7.1 and earlier allows remote attackers to cause a denial of service (infinite loop) of a collectd instance (configured with SecurityLevel None and with empty AuthFile options) via a crafted UDP packet.	collectd	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3944
3104	CVE-2017-7396	MEDIUM	High	In TigerVNC 1.7.1 (CConnection.cxx CConnection::CConnection), an unauthenticated client can cause a small memory leak in the server.	tigervnc	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3928
3105	CVE-2017-7395	MEDIUM	Medium	In TigerVNC 1.7.1 (SMsgReader.cxx SMsgReader::readClientCutText), by causing an integer overflow, an authenticated client can crash the server.	tigervnc	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3935
3106	CVE-2017-7394	MEDIUM	High	In TigerVNC 1.7.1 (SSecurityPlain.cxx SSecurityPlain::processMsg), unauthenticated users can crash the server by sending long usernames.	tigervnc	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3908
3107	CVE-2017-7393	MEDIUM	High	In TigerVNC 1.7.1 (VNCSConnectionST.cxx VNCSConnectionST::fence), an authenticated client can cause a double free, leading to denial of service or potentially code execution.	tigervnc	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3887
3108	CVE-2017-7392	MEDIUM	High	In TigerVNC 1.7.1 (SSecurityVeNCrypt.cxx SSecurityVeNCrypt::SSecurityVeNCrypt), an unauthenticated client can cause a small memory leak in the server.	tigervnc	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3969
3109	CVE-2017-7377	LOW	Medium	The (1) v9fs_create and (2) v9fs_lcreate functions in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allow local guest OS privileged users to cause a denial of service (file descriptor or memory consumption) via vectors related to an already in-use fid.	qemu	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3947

	A	B	C	D	E	F	G	H	I	J	K	L	M
3110	CVE-2017-7376	HIGH	CRITICAL	Buffer overflow in libxml2 allows remote attackers to execute arbitrary code by leveraging an incorrect limit for port values when handling redirects.	libxml2	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3315
3111	CVE-2017-7375	HIGH	CRITICAL	A flaw in libxml2 allows remote XML entity inclusion with default parser flags (i.e., when the caller did not request entity substitution, DTD validation, external DTD subset loading, or default DTD attributes). Depending on the context, this may expose a higher-risk attack surface in libxml2 not usually reachable with default parser flags, and expose content from local files, HTTP, or FTP servers (which might be otherwise unreachable).	libxml2	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3368
3112	CVE-2017-7374	HIGH	High	Use-after-free vulnerability in fs/crypto/ in the Linux kernel before 4.10.7 allows local users to cause a denial of service (NULL pointer dereference) or possibly gain privileges by revoking keyring keys being used for ext4, f2fs, or ubifs encryption, causing cryptographic transform objects to be freed prematurely.	linux	Unchanged	Not vulnerable	9.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3937
3113	CVE-2017-7346	MEDIUM	Medium	The vmw_gb_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.7 does not validate certain levels data, which allows local users to cause a denial of service (system hang) via a crafted ioctl call for a /dev/dri/renderD* device.	linux	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3958
3114	CVE-2017-7319			A vulnerability in the Linux kernel package 3.16.0-28 on Ubuntu 14.04 LTS allows any user to send a SIGIO signal to any process. If the process does not catch or ignore the signal, it will exit.	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3881
3115	CVE-2017-7308	HIGH	High	The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to cause a denial of service (overflow) or possibly have unspecified other impact via crafted system calls.	linux	Unchanged	8.0.0.17	9.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3904
3116	CVE-2017-7304	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read (of size 8) because of missing a check (in the copy_special_section_fields function) for an invalid sh_link field before attempting to follow it. This vulnerability causes Binutils utilities like strip to crash.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3961
3117	CVE-2017-7303	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to an invalid read (of size 4) because of missing a check (in the find_link function) for null headers before attempting to match them. This vulnerability causes Binutils utilities like strip to crash.	binutils	Unchanged	Not vulnerable	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3900
3118	CVE-2017-7302	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a swap_std_reloc_out function in bfd/aoutx.h that is vulnerable to an invalid read (of size 4) because of missing checks for relocs that could not be recognised. This vulnerability causes Binutils utilities like strip to crash.	binutils	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3888
3119	CVE-2017-7301	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an aout_link_add_symbols function in bfd/aoutx.h that has an off-by-one vulnerability because it does not carefully check the string offset. The vulnerability could lead to a GNU linker (ld) program crash.	binutils	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3950
3120	CVE-2017-7300	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an aout_link_add_symbols function in bfd/aoutx.h that is vulnerable to a heap-based buffer over-read (off-by-one) because of an incomplete check for invalid string offsets while loading symbols, leading to a GNU linker (ld) program crash.	binutils	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3941
3121	CVE-2017-7299	MEDIUM	Medium	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has an invalid read (of size 8) because the code to emit relocs (bfd_elf_final_link function in bfd/elflink.c) does not check the format of the input file before trying to read the ELF reloc section header. The vulnerability leads to a GNU linker (ld) program crash.	binutils	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3956
3122	CVE-2017-7294	HIGH	High	The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.6 does not validate addition of certain levels data, which allows local users to trigger an integer overflow and out-of-bounds write, and cause a denial of service (system hang or crash) or possibly gain privileges, via a crafted ioctl call for a /dev/dri/renderD* device.	linux	Unchanged	8.0.0.17	9.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3929
3123	CVE-2017-7286			The Linux kernel package 3.16.0-28 on Ubuntu 14.04 LTS mishandles a series of mmap system calls for /dev/zero with different starting addresses, with a stated impact of allowing for a local user to possibly gain root access, aka an inode integer overflow.	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3959
3124	CVE-2017-7277	MEDIUM	High	The TCP stack in the Linux kernel through 4.10.6 mishandles the SCM_TIMESTAMPING_OPT_STATS feature, which allows local users to obtain sensitive information from the kernel's internal socket data structures or cause a denial of service (out-of-bounds read) via crafted system calls, related to net/core/skbuff.c and net/socket.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3687
3125	CVE-2017-7275	MEDIUM	Medium	The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers to cause a denial of service (attempted large memory allocation and application crash) via a crafted file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8862 and CVE-2016-8866.	imagemagick	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3815

	A	B	C	D	E	F	G	H	I	J	K	L	M
3126	CVE-2017-7273	MEDIUM	Medium	The cp_report_fixup function in drivers/hid/hid-cypress.c in the Linux kernel 4.x before 4.9.4 allows physically proximate attackers to cause a denial of service (integer underflow) or possibly have unspecified other impact via a crafted HID report.	linux	Unchanged	8.0.0.16	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3717
3127	CVE-2017-7272	MEDIUM	High	PHP through 7.1.3 enables potential SSRF in applications that accept an fsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.	php	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3781
3128	CVE-2017-7261	MEDIUM	Medium	The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.5 does not check for a zero value of certain levels data, which allows local users to cause a denial of service (ZERO_SIZE_PTR dereference, and GPF and possibly panic) via a crafted ioctl call for a /dev/dri/renderD* device.	linux	Unchanged	8.0.0.23	9.0.0.11	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3664
3129	CVE-2017-7246	MEDIUM	High	Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 268) or possibly have unspecified other impact via a crafted file.	pcre	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3728
3130	CVE-2017-7245	MEDIUM	High	Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 4) or possibly have unspecified other impact via a crafted file.	pcre	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3774
3131	CVE-2017-7244	MEDIUM	Medium	The _pcre32_xclass function in pcre_xclass.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (invalid memory read) via a crafted file.	pcre	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3765
3132	CVE-2017-7227	MEDIUM	High	GNU linker (ld) in GNU Binutils 2.28 is vulnerable to a heap-based buffer overflow while processing a bogus input script, leading to a program crash. This relates to lack of '\0' termination of a name field in ldlex.l.	binutils	Unchanged	8.0.0.19	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3809
3133	CVE-2017-7226	MEDIUM	Critical	The pe_ILF_object_p function in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, is vulnerable to a heap-based buffer over-read of size 4049 because it uses the strlen function instead of strnlen, leading to program crashes in several utilities such as addr2line, size, and strings. It could lead to information disclosure as well.	binutils	Unchanged	8.0.0.19	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3640
3134	CVE-2017-7225	MEDIUM	High	The find_nearest_line function in addr2line in GNU Binutils 2.28 does not handle the case where the main file name and the directory name are both empty, triggering a NULL pointer dereference and an invalid write, and leading to a program crash.	binutils	Unchanged	8.0.0.19	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3735
3135	CVE-2017-7224	MEDIUM	Medium	The find_nearest_line function in objdump in GNU Binutils 2.28 is vulnerable to an invalid write (of size 1) while disassembling a corrupt binary that contains an empty function name, leading to a program crash.	binutils	Unchanged	8.0.0.19	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3721
3136	CVE-2017-7223	MEDIUM	High	GNU assembler in GNU Binutils 2.28 is vulnerable to a global buffer overflow (of size 1) while attempting to unget an EOF character from the input stream, potentially leading to a program crash.	binutils	Unchanged	8.0.0.19	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3710
3137	CVE-2017-7210	MEDIUM	Medium	objdump in GNU Binutils 2.28 is vulnerable to multiple heap-based buffer over-reads (of size 1 and size 8) while handling corrupt STABS enum type strings in a crafted object file, leading to program crash.	binutils	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3793
3138	CVE-2017-7209	MEDIUM	Medium	The dump_section_as_bytes function in readelf in GNU Binutils 2.28 accesses a NULL pointer while reading section contents in a corrupt binary, leading to a program crash.	binutils	Unchanged	Not vulnerable	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3817
3139	CVE-2017-7208	MEDIUM	High	The decode_residual function in libavcodec in libav 9.21 allows remote attackers to cause a denial of service (buffer over-read) or obtain sensitive information from process memory via a crafted h264 video file.	libav	Unchanged	8.0.0.18	9.0.0.6	10.17.41.3	10.18.44.1	Won't Fix	Won't Fix	LIN9-3812
3140	CVE-2017-7207	MEDIUM	Medium	The mem_get_bits_rectangle function in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted PostScript document.	ghostscript	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3736
3141	CVE-2017-7206	MEDIUM	High	The ff_h2645_extract_rbsp function in libavcodec in libav 9.21 allows remote attackers to cause a denial of service (heap-based buffer over-read) or obtain sensitive information from process memory via a crafted h264 video file.	libav	Unchanged	Not vulnerable	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3688
3142	CVE-2017-7191	HIGH	Critical	The netjoin processing in Irssi 1.x before 1.0.2 allows attackers to cause a denial of service (use-after-free) and possibly execute arbitrary code via unspecified vectors.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3787
3143	CVE-2017-7189	MEDIUM	HIGH	main/streams/xp_socket.c in PHP 7.x before 2017-03-07 misparses fsockopen calls, such as by interpreting fsockopen('127.0.0.1:80', 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hardcoded into an application as a security policy, but the hostname argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input.	php	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	LIN1018-4419
3144	CVE-2017-7187	HIGH	High	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_LEN ioctl call, leading to out-of-bounds write access in the sg_write function.	linux	Unchanged	8.0.0.17	9.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3816
3145	CVE-2017-7186	MEDIUM	High	libpcre1 in PCRE 8.40 and libpcre2 in PCRE2 10.23 allow remote attackers to cause a denial of service (segmentation violation for read access, and application crash) by triggering an invalid Unicode property lookup.	pcre	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3671

	A	B	C	D	E	F	G	H	I	J	K	L	M
3146	CVE-2017-7184	HIGH	High	The linux-image-* package 4.8.0.41.52 for the Linux kernel on Ubuntu 16.10 allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) via unspecified vectors, as demonstrated during a Pwn2Own competition at CanSecWest 2017.	linux	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4209
3147	CVE-2017-7177	MEDIUM	High	Suricata before 3.2.1 has an IPv4 defragmentation evasion issue caused by lack of a check for the IP protocol during fragment matching.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3655
3148	CVE-2017-6969	MEDIUM	Critical	readelf in GNU Binutils 2.28 is vulnerable to a heap-based buffer over-read while processing corrupt RL78 binaries. The vulnerability can trigger program crashes. It may lead to an information leak as well.	binutils	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3709
3149	CVE-2017-6966	MEDIUM	Medium	readelf in GNU Binutils 2.28 has a use-after-free (specifically read-after-free) error while processing multiple, relocated sections in an MSP430 binary. This is caused by mishandling of an invalid symbol index, and mishandling of state across invocations.	binutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3639
3150	CVE-2017-6965	MEDIUM	Medium	readelf in GNU Binutils 2.28 writes to illegal addresses while processing corrupt input files containing symbol-difference relocations, leading to a heap-based buffer overflow.	binutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3682
3151	CVE-2017-6964	HIGH	High	dmcrypt-get-device, as shipped in the eject package of Debian and Ubuntu, does not check the return value of the (1) setuid or (2) setgid function, which might cause dmcrypt-get-device to execute code, which was intended to run as an unprivileged user, as root. This affects eject through 2.1.5+deb1+cvs20081104-13.1 on Debian, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.10.1 on Ubuntu 16.10, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.04.1 on Ubuntu 16.04 LTS, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.14.04.1 on Ubuntu 14.04 LTS, and eject before 2.1.5+deb1+cvs20081104-9ubuntu0.1 on Ubuntu 12.04 LTS.	eject	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3686
3152	CVE-2017-6951	MEDIUM	Medium	The keyring_search_aux function in security/keys/keyring.c in the Linux kernel through 3.14.79 allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a request_key system call for the dead type.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3789
3153	CVE-2017-6892	MEDIUM	High	In libsndfile version 1.0.28, an error in the aiff_read_chanmap() function (aiff.c) can be exploited to cause an out-of-bounds read memory access via a specially crafted AIFF file.	libsndfile	Unchanged	8.0.0.19	9.0.0.8	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-4420
3154	CVE-2017-6891	MEDIUM	High	Two errors in the asn1_find_node() function (lib/parser_aux.c) within GnuTLS libtasn1 version 4.10 can be exploited to cause a stacked-based buffer overflow by tricking a user into processing a specially crafted assignments file via the e.g. asn1Coding utility.	gnutls&libtasn1	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4295
3155	CVE-2017-6888	MEDIUM	MEDIUM	An error in the read_metadata_vorbiscomment_() function (src/libFLAC/stream_decoder.c) in FLAC version 1.3.2 can be exploited to cause a memory leak via a specially crafted FLAC file.	flac	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-3873
3156	CVE-2017-6874	MEDIUM	High	Race condition in kernel/ucount.c in the Linux kernel through 4.10.2 allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via crafted system calls that leverage certain decrement behavior that causes incorrect interaction between put_ucounts and get_ucounts.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3705
3157	CVE-2017-6852	MEDIUM	High	Heap-based buffer overflow in the jpc_dec_decodepkt function in jpc_t2dec.c in JasPer 2.0.10 allows remote attackers to have unspecified impact via a crafted image.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3677
3158	CVE-2017-6851	MEDIUM	Medium	The jas_matrix_bindsub function in jas_seq.c in JasPer 2.0.10 allows remote attackers to cause a denial of service (invalid read) via a crafted image.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3811
3159	CVE-2017-6850	MEDIUM	Medium	The jp2_cdef_destroy function in jp2_cod.c in JasPer before 2.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted image.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3755
3160	CVE-2017-6839	MEDIUM	Medium	Integer overflow in modules/MSADPCM.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3822
3161	CVE-2017-6838	MEDIUM	Medium	Integer overflow in sfcommands/sfconvert.c in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3754
3162	CVE-2017-6837	MEDIUM	Medium	WAVE.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via vectors related to a large number of coefficients.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3642
3163	CVE-2017-6836	MEDIUM	Medium	Heap-based buffer overflow in the Expand3To4Module::run function in libaudiofile/modules/SimpleModule.h in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3643
3164	CVE-2017-6835	MEDIUM	Medium	The reset1 function in libaudiofile/modules/BlockCodec.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (divide-by-zero error and crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3726
3165	CVE-2017-6834	MEDIUM	Medium	Heap-based buffer overflow in the ulaw2linear_buf function in G711.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3794
3166	CVE-2017-6833	MEDIUM	Medium	The runPull function in libaudiofile/modules/BlockCodec.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (divide-by-zero error and crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3742
3167	CVE-2017-6832	MEDIUM	Medium	Heap-based buffer overflow in the decodeBlock in MSADPCM.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3740

	A	B	C	D	E	F	G	H	I	J	K	L	M
3168	CVE-2017-6831	MEDIUM	Medium	Heap-based buffer overflow in the decodeBlockWAVE function in IMA.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3706
3169	CVE-2017-6830	MEDIUM	Medium	Heap-based buffer overflow in the alaw2linear_buf function in G711.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3741
3170	CVE-2017-6829	MEDIUM	Medium	The decodeSample function in IMA.cpp in Audio File Library (aka audiofile) 0.3.6 allows remote attackers to cause a denial of service (crash) via a crafted file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3679
3171	CVE-2017-6828	MEDIUM	High	Heap-based buffer overflow in the readValue function in FileHandle.cpp in audiofile (aka libaudiofile and Audio File Library) 0.3.6 allows remote attackers to have unspecified impact via a crafted WAV file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3799
3172	CVE-2017-6827	MEDIUM	High	Heap-based buffer overflow in the MSADPCM::initializeCoefficients function in MSADPCM.cpp in audiofile (aka libaudiofile and Audio File Library) 0.3.6 allows remote attackers to have unspecified impact via a crafted audio file.	audiofile	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3685
3173	CVE-2017-6519	MEDIUM	Critical	avahi-daemon in Avahi through 0.6.32 inadvertently responds to IPv6 unicast queries with source addresses that are not on-link, which allows remote attackers to cause a denial of service (traffic amplification) or obtain potentially sensitive information via port-5353 UDP packets. NOTE: this may overlap CVE-2015-2809.	avahi	Unchanged	Investigate	Investigate	Investigate	Investigate	10.19.45.1	Not vulnerable	LIN1018-3493
3174	CVE-2017-6508	MEDIUM	Medium	CRLF injection vulnerability in the url_parse function in url.c in Wget through 1.19.1 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in the host subcomponent of a URL.	wget	Unchanged	8.0.0.16	9.0.0.5	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3519
3175	CVE-2017-6505	LOW	Medium	The ohci_service_ed_list function in hw/usb/hcd-ohci.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (infinite loop) via vectors involving the number of link endpoint list descriptors.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3803
3176	CVE-2017-6502	MEDIUM	Medium	An issue was discovered in ImageMagick 6.9.7. A specially crafted webp file could lead to a file-descriptor leak in libmagickcore (thus, a DoS).	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3500
3177	CVE-2017-6501	MEDIUM	Medium	An issue was discovered in ImageMagick 6.9.7. A specially crafted xcf file could lead to a NULL pointer dereference.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3509
3178	CVE-2017-6500	MEDIUM	Medium	An issue was discovered in ImageMagick 6.9.7. A specially crafted sun file triggers a heap-based buffer over-read.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3533
3179	CVE-2017-6499	MEDIUM	Medium	An issue was discovered in Magick++ in ImageMagick 6.9.7. A specially crafted file creating a nested exception could lead to a memory leak (thus, a DoS).	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3588
3180	CVE-2017-6498	MEDIUM	Medium	An issue was discovered in ImageMagick 6.9.7. Incorrect TGA files could trigger assertion failures, thus leading to DoS.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3510
3181	CVE-2017-6497	MEDIUM	High	An issue was discovered in ImageMagick 6.9.7. A specially crafted psd file could lead to a NULL pointer dereference (thus, a DoS).	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3534
3182	CVE-2017-6474	MEDIUM	High	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a NetScaler file parser infinite loop, triggered by a malformed capture file. This was addressed in wiretap/netscaler.c by validating record sizes.	wireshark	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3508
3183	CVE-2017-6473	MEDIUM	High	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a K12 file parser crash, triggered by a malformed capture file. This was addressed in wiretap/k12.c by validating the relationships between lengths and offsets.	wireshark	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3587
3184	CVE-2017-6472	MEDIUM	High	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is an RTMPT dissector infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-rtmpt.c by properly incrementing a certain sequence value.	wireshark	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3520
3185	CVE-2017-6471	MEDIUM	High	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a WSP infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-wsp.c by validating the capability length.	wireshark	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3507
3186	CVE-2017-6470	HIGH	High	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is an IAX2 infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-iax2.c by constraining packet lateness.	wireshark	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3527
3187	CVE-2017-6469	MEDIUM	High	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is an LDSS dissector crash, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-ldss.c by ensuring that memory is allocated for a certain data structure.	wireshark	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3536
3188	CVE-2017-6468	MEDIUM	High	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a NetScaler file parser crash, triggered by a malformed capture file. This was addressed in wiretap/netscaler.c by validating the relationship between pages and records.	wireshark	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3584
3189	CVE-2017-6467	MEDIUM	High	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a Netscaler file parser infinite loop, triggered by a malformed capture file. This was addressed in wiretap/netscaler.c by changing the restrictions on file size.	wireshark	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3537
3190	CVE-2017-6464	MEDIUM	Medium	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote attackers to cause a denial of service (ntpd crash) via a malformed mode configuration directive.	ntp	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3616
3191	CVE-2017-6463	MEDIUM	Medium	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote authenticated users to cause a denial of service (daemon crash) via an invalid setting in a :config directive, related to the unpeer option.	ntp	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3618
3192	CVE-2017-6462	MEDIUM	High	Buffer overflow in the legacy Datum Programmable Time Server (DPTS) refclock driver in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via a crafted /dev/datum device.	ntp	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3617

	A	B	C	D	E	F	G	H	I	J	K	L	M
3193	CVE-2017-6460	MEDIUM	High	Stack-based buffer overflow in the resIist function in ntpq in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote servers have unspecified impact via a long flagstr variable in a restriction list response.	ntp	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3624
3194	CVE-2017-6459	LOW	Medium	The Windows installer for NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via vectors related to an argument with multiple null bytes.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3621
3195	CVE-2017-6458	MEDIUM	High	Multiple buffer overflows in the ctl_put* functions in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allow remote authenticated users to have unspecified impact via a long variable.	ntp	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3622
3196	CVE-2017-6455	MEDIUM	High	NTP before 4.2.8p10 and 4.3.x before 4.3.94, when using PPSAPI, allows local users to gain privileges via a DLL in the PPSAPI_DLLS environment variable.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3619
3197	CVE-2017-6452	MEDIUM	High	Stack-based buffer overflow in the Windows installer for NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via an application path on the command line.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3620
3198	CVE-2017-6451	MEDIUM	High	The mx4200_send function in the legacy MX4200 refclock in NTP before 4.2.8p10 and 4.3.x before 4.3.94 does not properly handle the return value of the snprintf function, which allows local users to execute arbitrary code via unspecified vectors, which trigger an out-of-bounds memory write.	ntp	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3623
3199	CVE-2017-6440	LOW	Medium	The parse_data_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (memory allocation error) via a crafted plist file.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3648
3200	CVE-2017-6439	LOW	Medium	Heap-based buffer overflow in the parse_string_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (out-of-bounds write) via a crafted plist file.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3776
3201	CVE-2017-6438	MEDIUM	High	Heap-based buffer overflow in the parse_unicode_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (out-of-bounds write) and possibly code execution via a crafted plist file.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3730
3202	CVE-2017-6437	LOW	Medium	The base64encode function in base64.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (out-of-bounds read) via a crafted plist file.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3698
3203	CVE-2017-6436	LOW	Medium	The parse_string_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (memory allocation error) via a crafted plist file.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3756
3204	CVE-2017-6435	LOW	Medium	The parse_string_node function in bplist.c in libimobiledevice libplist 1.12 allows local users to cause a denial of service (memory corruption) via a crafted plist file.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3788
3205	CVE-2017-6429	MEDIUM	High	Buffer overflow in the tcpcapinfo utility in Tcpreplay before 4.2.0 Beta 1 allows remote attackers to have unspecified impact via a pcap file with an over-size packet.	tcpreplay	Unchanged	Not vulnerable	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3780
3206	CVE-2017-6420	Medium	Medium	The wwunpack function in libclamav/wwunpack.c in ClamAV 0.99.2 allows remote attackers to cause a denial of service (use-after-free) via a crafted PE file with WWPack compression.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4994
3207	CVE-2017-6419	Medium	High	mspack/lzxd.c in libmspack 0.5alpha, as used in ClamAV 0.99.2, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted CHM file.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5091
3208	CVE-2017-6418	Medium	Medium	libclamav/message.c in ClamAV 0.99.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted e-mail message.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4976
3209	CVE-2017-6363	MEDIUM	HIGH	** DISPUTED ** In the GD Graphics Library (aka LibGD) through 2.2.5, there is a heap-based buffer over-read in tiffWriter in gd_tiff.c. NOTE: the vendor says In my opinion this issue should not have a CVE, since the GD and GD2 formats are documented to be 'obsolete, and should only be used for development and testing purposes.'	gd	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.6	Vulnerable	LIN1019-4099
3210	CVE-2017-6353	MEDIUM	Medium	net/sctp/socket.c in the Linux kernel through 4.10.1 does not properly restrict association peel-off operations during certain wait states, which allows local users to cause a denial of service (invalid unlock and double free) via a multithreaded application. NOTE: this vulnerability exists because of an incorrect fix for CVE-2017-5986.	linux	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3549
3211	CVE-2017-6350	HIGH	Critical	An integer overflow at an unserialize_uep memory allocation site would occur for vim before patch 8.0.0378, if it does not properly validate values for tree length when reading a corrupted undo file, which may lead to resultant buffer overflows.	vim	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3551
3212	CVE-2017-6349	HIGH	Critical	An integer overflow at a u_read_undo memory allocation site would occur for vim before patch 8.0.0377, if it does not properly validate values for tree length when reading a corrupted undo file, which may lead to resultant buffer overflows.	vim	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3503
3213	CVE-2017-6348	MEDIUM	Medium	The hashbin_delete function in net/irda/irqueue.c in the Linux kernel before 4.9.13 improperly manages lock dropping, which allows local users to cause a denial of service (deadlock) via crafted operations on IrDA devices.	linux	Unchanged	8.0.0.16	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3532
3214	CVE-2017-6347	HIGH	High	The ip_cmsg_recv_checksum function in net/ipv4/ip_sockglue.c in the Linux kernel before 4.10.1 has incorrect expectations about skb data layout, which allows local users to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted system calls, as demonstrated by use of the MSG_MORE flag in conjunction with loopback UDP transmission.	linux	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3581
3215	CVE-2017-6346	MEDIUM	High	Race condition in net/packet/af_packet.c in the Linux kernel before 4.9.13 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a multithreaded application that makes PACKET_FANOUT setsockopt system calls.	linux	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3511

	A	B	C	D	E	F	G	H	I	J	K	L	M
3216	CVE-2017-6345	MEDIUM	High	The LLC subsystem in the Linux kernel before 4.9.13 does not ensure that a certain destructor exists in required circumstances, which allows local users to cause a denial of service (BUG_ON) or possibly have unspecified other impact via crafted system calls.	linux	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3580
3217	CVE-2017-6314	MEDIUM	Medium	The make_available_at_least function in io-tiff.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (infinite loop) via a large TIFF file.	gdk-pixbuf	Unchanged	8.0.0.25	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3530
3218	CVE-2017-6313	MEDIUM	Medium	Integer underflow in the load_resources function in io-icns.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (out-of-bounds read and program crash) via a crafted image entry size in an ICO file.	gdk-pixbuf	Unchanged	8.0.0.25	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3568
3219	CVE-2017-6312	MEDIUM	Medium	Integer overflow in io-ico.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (segmentation fault and application crash) via a crafted image entry offset in an ICO file, which triggers an out-of-bounds read, related to compiler optimizations.	gdk-pixbuf	Unchanged	8.0.0.25	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3567
3220	CVE-2017-6311	MEDIUM	High	gdk-pixbuf-thumbnailer.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors related to printing an error message.	gdk-pixbuf	Unchanged	8.0.0.25	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3528
3221	CVE-2017-6214	MEDIUM	High	The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag.	linux	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3409
3222	CVE-2017-6196	MEDIUM	High	Multiple use-after-free vulnerabilities in the gx_image_enum_begin function in base/gximage.c in Ghostscript before ecceafe3abba2714ef9b432035fe0739d9b1a283 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PostScript document.	ghostscript	Unchanged	8.0.0.26	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3385
3223	CVE-2017-6181	MEDIUM	High	The parse_char_class function in regparse.c in the Onigmo (aka Oniguruma-mod) regular expression library, as used in Ruby 2.4.0, allows remote attackers to cause a denial of service (deep recursion and application crash) via a crafted regular expression.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3911
3224	CVE-2017-6076	LOW	Medium	In versions of wolfSSL before 3.10.2 the function fp_mul_comba makes it easier to extract RSA key information for a malicious user who has access to view cache on a machine.	wolfssl	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3405
3225	CVE-2017-6074	HIGH	High	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.	linux	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3353
3226	CVE-2017-6058	MEDIUM	High	Buffer overflow in NetRxPkt::ehdr_buf in hw/net/net_rx_pkt.c in QEMU (aka Quick Emulator), when the VLANSTRIP feature is enabled on the vmxnet3 device, allows remote attackers to cause a denial of service (out-of-bounds access and QEMU process crash) via vectors related to VLAN stripping.	qemu	Unchanged	Not vulnerable	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3747
3227	CVE-2017-6014	HIGH	High	In Wireshark 2.2.4 and earlier, a crafted or malformed STANAG 4607 capture file will cause an infinite loop and memory exhaustion. If the packet size field in a packet header is null, the offset to read from will not advance, causing continuous attempts to read the same zero length packet. This will quickly exhaust all system memory.	wireshark	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3377
3228	CVE-2017-6004	MEDIUM	High	The compile_bracket_matchingpath function in pcre_jit_compile.c in PCRE through 8.x before revision 1680 (e.g., the PHP 7.1.1 bundled version) allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted regular expression.	pcre	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3387
3229	CVE-2017-6001	HIGH	High	Race condition in kernel/events/core.c in the Linux kernel before 4.9.7 allows local users to gain privileges via a crafted application that makes concurrent perf_event_open system calls for moving a software group into a hardware context. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-6786.	linux	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3386
3230	CVE-2017-5987	LOW	Medium	The sdhci_sdma_transfer_multi_blocks function in hw/sd/sdhci.c in QEMU (aka Quick Emulator) allows local OS guest privileged users to cause a denial of service (infinite loop and QEMU process crash) via vectors involving the transfer mode register during multi block transfer.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3712
3231	CVE-2017-5986	HIGH	Medium	Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allows local users to cause a denial of service (assertion failure and panic) via a multithreaded application that peels off an association in a certain buffer-full state.	linux	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3429
3232	CVE-2017-5985	LOW	Low	lxc-user-nic in Linux Containers (LXC) allows local users with a lxc-usernet allocation to create network interfaces on the host and choose the name of those interfaces by leveraging lack of netns ownership check.	lxc	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3678
3233	CVE-2017-5984	Medium	MEDIUM	In libavcodec in Libav 9.21, ff_h264_execute_ref_pic_marking() has a heap-based buffer over-read.	libav	Unchanged	Vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN8-10956
3234	CVE-2017-5973	LOW	Medium	The xhci_kick_epctx function in hw/usb/hcd-xhci.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (infinite loop and QEMU process crash) via vectors related to control transfer descriptor sequence.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3673

	A	B	C	D	E	F	G	H	I	J	K	L	M
3235	CVE-2017-5972	HIGH	High	The TCP stack in the Linux kernel 3.x does not properly implement a SYN cookie protection mechanism for the case of a fast network connection, which allows remote attackers to cause a denial of service (CPU consumption) by sending many TCP SYN packets, as demonstrated by an attack against the kernel-3.10.0 package in CentOS Linux 7.	linux	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3379
3236	CVE-2017-5970	MEDIUM	High	The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options.	linux	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3395
3237	CVE-2017-5969	LOW	Medium	libxml2 2.9.4, when used in recover mode, allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted XML document. NOTE: The maintainer states "I would disagree of a CVE with the Recover parsing option which should only be used for manual recovery at least for XML parser."	libxmi2	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4386
3238	CVE-2017-5967	LOW	Medium	The time subsystem in the Linux kernel through 4.9.9, when CONFIG_TIMER_STATS is enabled, allows local users to discover real PID values (as distinguished from PID values inside a PID namespace) by reading the /proc/timer_list file, related to the print_timer function in kernel/time/timer_list.c and the __timer_stats_timer_set_start_info function in kernel/time/timer.c.	linux	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3408
3239	CVE-2017-5953	HIGH	Critical	vim before patch 8.0.0322 does not properly validate values for tree length when handling a spell file, which may result in an integer overflow at a memory allocation site and a resultant buffer overflow.	vim	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3393
3240	CVE-2017-5951	MEDIUM	Medium	The mem_get_bits_rectangle function in base/gdevmem.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file.	ghostscript	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3932
3241	CVE-2017-5950	MEDIUM	Medium	The SingleDocParser::HandleNode function in yaml-cpp (aka LibYaml-C++) 0.5.3 allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted YAML file.	libyaml	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3878
3242	CVE-2017-5946	HIGH	Critical	The Zip::File component in the rubyzip gem before 1.2.1 for Ruby has a directory traversal vulnerability. If a site allows uploading of .zip files, an attacker can upload a malicious file that uses ../ pathname substrings to write arbitrary files to the filesystem.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3539
3243	CVE-2017-5932	MEDIUM	High	The path autocompletion feature in Bash 4.4 allows local users to gain privileges via a crafted filename starting with a (double quote) character and a command substitution metacharacter.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3753
3244	CVE-2017-5931	HIGH	High	Integer overflow in hw/virtio/virtio-crypto.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (QEMU process crash) or possibly execute arbitrary code on the host via a crafted virtio-crypto request, which triggers a heap-based buffer overflow.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3790
3245	CVE-2017-5898	LOW	Medium	Integer overflow in the emulated_apdu_from_guest function in usb/dev-smartcard-reader.c in Quick Emulator (Qemu), when built with the CCID Card device emulator support, allows local users to cause a denial of service (application crash) via a large Application Protocol Data Units (APDU) unit.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3715
3246	CVE-2017-5897	HIGH	Critical	The ip6gre_err function in net/ipv6/ip6_gre.c in the Linux kernel allows remote attackers to have unspecified impact via vectors involving GRE flags in an IPv6 packet, which trigger an out-of-bounds access.	linux	Unchanged	8.0.0.16	9.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3752
3247	CVE-2017-5857	MEDIUM	Medium	Memory leak in the virgl_cmd_resource_unref function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_UNREF commands sent without detaching the backing storage beforehand.	qemu	Unchanged	Not vulnerable	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3824
3248	CVE-2017-5856	MEDIUM	Medium	Memory leak in the megasas_handle_dcmd function in hw/scsi/megasas.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption) via MegaRAID Firmware Interface (MFI) commands with the sglist size set to a value over 2 Gb.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3722
3249	CVE-2017-5848	MEDIUM	High	The gst_ps_demux_parse_psm function in gst/mpegdemux/gstmpegdemux.c in gst-plugins-bad in GStreamer allows remote attackers to cause a denial of service (invalid memory read and crash) via vectors involving PSM parsing.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3417
3250	CVE-2017-5847	MEDIUM	High	The gst_asf_demux_process_ext_content_desc function in gst/asfdemux/gstasfdemux.c in gst-plugins-ugly in GStreamer allows remote attackers to cause a denial of service (out-of-bounds heap read) via vectors involving extended content descriptors.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3399
3251	CVE-2017-5846	MEDIUM	Medium	The gst_asf_demux_process_ext_stream_pro ps function in gst/asfdemux/gstasfdemux.c in gst-plugins-ugly in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (invalid memory read and crash) via vectors related to the number of languages in a video file.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3397
3252	CVE-2017-5845	MEDIUM	High	The gst_avi_demux_parse_ncdt function in gst/avi/gstavidemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (invalid memory read and crash) via a ncdt sub-tag that goes behind the surrounding tag.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3420

	A	B	C	D	E	F	G	H	I	J	K	L	M
3253	CVE-2017-5844	MEDIUM	Medium	The gst_riff_create_audio_caps function in gst-libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (floating point exception and crash) via a crafted ASF file.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3396
3254	CVE-2017-5843	MEDIUM	High	Multiple use-after-free vulnerabilities in the (1) gst_mini_object_unref, (2) gst_tag_list_unref, and (3) gst_mxf_demux_update_essence_tracks functions in GStreamer before 1.10.3 allow remote attackers to cause a denial of service (crash) via vectors involving stream tags, as demonstrated by 02785736.mxf.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3384
3255	CVE-2017-5842	MEDIUM	Medium	The html_context_handle_element function in gst/subparse/samiparse.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted SMI file, as demonstrated by OneNote_Manager.smi.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3416
3256	CVE-2017-5841	MEDIUM	High	The gst_avi_demux_parse_ncdt function in gst/avi/gstavidemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds heap read) via vectors involving ncdt tags.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3382
3257	CVE-2017-5840	MEDIUM	High	The qtdemux_parse_samples function in gst/isomp4/qtdemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds heap read) via vectors involving the current stts index.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3398
3258	CVE-2017-5839	MEDIUM	High	The gst_riff_create_audio_caps function in gst-libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 does not properly limit recursion, which allows remote attackers to cause a denial of service (stack overflow and crash) via vectors involving nested WAVEFORMATEX.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3390
3259	CVE-2017-5838	MEDIUM	High	The gst_date_time_new_from_iso8601_string function in gst/gstdatetime.c in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a malformed datetime string.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3402
3260	CVE-2017-5837	MEDIUM	Medium	The gst_riff_create_audio_caps function in gst-libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (floating point exception and crash) via a crafted video file.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3425
3261	CVE-2017-5836	MEDIUM	High	The plist_free_data function in plist.c in libplist allows attackers to cause a denial of service (crash) via vectors involving an integer node that is treated as a PLIST_KEY and then triggers an invalid free.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3562
3262	CVE-2017-5835	MEDIUM	High	libplist allows attackers to cause a denial of service (large memory allocation and crash) via vectors involving an offset size of zero.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3524
3263	CVE-2017-5834	MEDIUM	Medium	The parse_dict_node function in bplist.c in libplist allows attackers to cause a denial of service (out-of-bounds heap read and crash) via a crafted file.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3575
3264	CVE-2017-5754	MEDIUM	Medium	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache. (Spectre / Meltdown)	linux	Unchanged	8.0.0.26	9.0.0.20	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2987
3265	CVE-2017-5753	MEDIUM	Medium	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. (Spectre / Meltdown)	linux	Unchanged	8.0.0.29	9.0.0.18	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2986
3266	CVE-2017-5715	MEDIUM	Medium	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. (Spectre / Meltdown)	linux	Unchanged	8.0.0.29	9.0.0.18	10.17.41.14	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2989
3267	CVE-2017-5669	MEDIUM	High	The do_shmat function in ipc/shm.c in the Linux kernel through 4.9.12 does not restrict the address calculated by a certain rounding operation, which allows local users to map page zero, and consequently bypass a protection mechanism that exists for the mmap system call, by making crafted shmget and shmat system calls in a privileged context.	linux	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3400
3268	CVE-2017-5667	LOW	Medium	The sdhci_sdma_transfer_multi_blocks function in hw/sd/sdhci.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (out-of-bounds heap access and crash) or execute arbitrary code on the QEMU host via vectors involving the data transfer length.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3785
3269	CVE-2017-5645	HIGH	Critical	In Apache Log4j 2.x before 2.8.2, when using the TCP socket server or UDP socket server to receive serialized log events from another application, a specially crafted binary payload can be sent that, when deserialized, can execute arbitrary code.	log4j1.2	Unchanged	8.0.0.33	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-12023
3270	CVE-2017-5618	HIGH	High	GNU screen before 4.5.1 allows local users to modify arbitrary files and consequently gain root privileges by leveraging improper checking of logfile permissions.	screen	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3657
3271	CVE-2017-5601	MEDIUM	High	An error in the lha_read_file_header_1() function (archive_read_support_format_lha.c) in libarchive 3.2.2 allows remote attackers to trigger an out-of-bounds read memory access and subsequently cause a crash via a specially crafted archive.	libarchive	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3220
3272	CVE-2017-5597	MEDIUM	High	In Wireshark 2.2.0 to 2.2.3 and 2.0.0 to 2.0.9, the DHCPv6 dissector could go into a large loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-dhcpv6.c by changing a data type to avoid an integer overflow.	wireshark	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3244

	A	B	C	D	E	F	G	H	I	J	K	L	M
3273	CVE-2017-5596	MEDIUM	High	In Wireshark 2.2.0 to 2.2.3 and 2.0.0 to 2.0.9, the ASTERIX dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-asterix.c by changing a data type to avoid an integer overflow.CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')	wireshark	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3157
3274	CVE-2017-5581	MEDIUM	Critical	Buffer overflow in the ModifiablePixelBuffer::fillRect function in TigerVNC before 1.7.1 allows remote servers to execute arbitrary code via an RRE message with subrectangle outside framebuffer boundaries.	tigervnc	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3560
3275	CVE-2017-5579	MEDIUM	Medium	Memory leak in the serial_exit_core function in hw/char/serial.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3733
3276	CVE-2017-5578	MEDIUM	Medium	Memory leak in the virtio_gpu_resource_attach_backing function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_ATTACH_BACKING commands.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3750
3277	CVE-2017-5577	MEDIUM	Medium	The vc4_get_bcl function in drivers/gpu/drm/vc4/vc4_gem.c in the VideoCore DRM driver in the Linux kernel before 4.9.7 does not set an errno value upon certain overflow detections, which allows local users to cause a denial of service (incorrect pointer dereference and OOPS) via inconsistent size values in a VC4_SUBMIT_CL ioctl call.	linux	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3208
3278	CVE-2017-5576	HIGH	High	Integer overflow in the vc4_get_bcl function in drivers/gpu/drm/vc4/vc4_gem.c in the VideoCore DRM driver in the Linux kernel before 4.9.7 allows local users to cause a denial of service or possibly have unspecified other impact via a crafted size value in a VC4_SUBMIT_CL ioctl call.	linux	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3273
3279	CVE-2017-5563	MEDIUM	High	LibTIFF version 4.0.7 is vulnerable to a heap-based buffer over-read in tif_lzw.c resulting in DoS or code execution via a crafted bmp image to tools/bmp2tiff.	libtiff	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3256
3280	CVE-2017-5552	MEDIUM	Medium	Memory leak in the virgl_resource_attach_backing function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_ATTACH_BACKING commands.	qemu	Unchanged	Not vulnerable	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3806
3281	CVE-2017-5551	LOW	Medium	The simple_set_acl function in fs/posix_acl.c in the Linux kernel before 4.9.6 preserves the setgid bit during a setxattr call involving a tmpfs filesystem, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-7097.	linux	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3240
3282	CVE-2017-5550	LOW	Medium	Off-by-one error in the pipe_advance function in lib/iov_iter.c in the Linux kernel before 4.9.5 allows local users to obtain sensitive information from uninitialized heap-memory locations in opportunistic circumstances by reading from a pipe after an incorrect buffer-release decision.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3295
3283	CVE-2017-5549	LOW	Medium	The klsi_105_get_line_state function in drivers/usb/serial/kl5kusb105.c in the Linux kernel before 4.9.5 places uninitialized heap-memory contents into a log entry upon a failure to read the line status, which allows local users to obtain sensitive information by reading the log.	linux	Unchanged	8.0.0.15	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3180
3284	CVE-2017-5548	HIGH	High	drivers/net/ieee802154/atusb.c in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3246
3285	CVE-2017-5547	HIGH	High	drivers/hid/hid-corsair.c in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3219
3286	CVE-2017-5546	HIGH	High	The freelist-randomization feature in mm/slab.c in the Linux kernel 4.8.x and 4.9.x before 4.9.5 allows local users to cause a denial of service (duplicate freelist entries and system crash) or possibly have unspecified other impact in opportunistic circumstances by leveraging the selection of a large value for a random number.	linux	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3297
3287	CVE-2017-5545	MEDIUM	Critical	The main function in plistutil.c in libimobiledevice libplist through 1.12 allows attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read) via Apple Property List data that is too short.	libplist	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3230
3288	CVE-2017-5526	MEDIUM	Medium	Memory leak in hw/audio/es1370.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3672
3289	CVE-2017-5525	MEDIUM	Medium	Memory leak in hw/audio/ac97.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3821

	A	B	C	D	E	F	G	H	I	J	K	L	M
3290	CVE-2017-5511	HIGH	Critical	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact by leveraging an improper cast, which triggers a heap-based buffer overflow.	imagemagick	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3762
3291	CVE-2017-5510	MEDIUM	High	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact via a crafted PSD file, which triggers an out-of-bounds write.	imagemagick	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3647
3292	CVE-2017-5509	MEDIUM	High	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact via a crafted PSD file, which triggers an out-of-bounds write.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3734
3293	CVE-2017-5508	MEDIUM	Medium	Heap-based buffer overflow in the PushQuantumPixel function in ImageMagick before 6.9.7-3 and 7.x before 7.0.4-3 allows remote attackers to cause a denial of service (application crash) via a crafted TIFF file.	imagemagick	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3823
3294	CVE-2017-5507	HIGH	High	Memory leak in coders/mpc.c in ImageMagick before 6.9.7-4 and 7.x before 7.0.4-4 allows remote attackers to cause a denial of service (memory consumption) via vectors involving a pixel cache.	imagemagick	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3819
3295	CVE-2017-5506	MEDIUM	High	Double free vulnerability in magick/profile.c in ImageMagick allows remote attackers to have unspecified impact via a crafted file.	imagemagick	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3694
3296	CVE-2017-5505	MEDIUM	Medium	The jas_matrix_asl function in jas_seq.c in JasPer 1.900.27 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted image.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3696
3297	CVE-2017-5504	MEDIUM	Medium	The jpc_undo_roi function in libjasper/jpc/jpc_dec.c in JasPer 1.900.27 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted image.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3583
3298	CVE-2017-5503	MEDIUM	Medium	The dec_clnpass function in libjasper/jpc/jpc_t1dec.c in JasPer 1.900.27 allows remote attackers to cause a denial of service (invalid memory write and crash) or possibly have unspecified other impact via a crafted image.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3535
3299	CVE-2017-5502	MEDIUM	Medium	libjasper/jp2/jp2_dec.c in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3513
3300	CVE-2017-5501	MEDIUM	Medium	Integer overflow in libjasper/jpc/jpc_tsfb.c in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via a crafted file.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3540
3301	CVE-2017-5500	MEDIUM	Medium	libjasper/jpc/jpc_dec.c in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3550
3302	CVE-2017-5499	MEDIUM	Medium	Integer overflow in libjasper/jpc/jpc_dec.c in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via a crafted file.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3543
3303	CVE-2017-5498	MEDIUM	Medium	libjasper/include/jasper/jas_math.h in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3546
3304	CVE-2017-5495	HIGH	High	All versions of Quagga, 0.93 through 1.1.0, are vulnerable to an unbounded memory allocation in the telnet 'vty' CLI, leading to a Denial-of-Service of Quagga daemons, or even the entire host. When Quagga daemons are configured with their telnet CLI enabled, anyone who can connect to the TCP ports can trigger this vulnerability, prior to authentication. Most distributions restrict the Quagga telnet interface to local access only by default. The Quagga telnet interface 'vty' input buffer grows automatically, without bound, so long as a newline is not entered. This allows an attacker to cause the Quagga daemon to allocate unbounded memory by sending very long strings without a newline. Eventually the daemon is terminated by the system, or the system itself runs out of memory. This is fixed in Quagga 1.1.1 and Free Range Routing (FRR) Protocol Suite 2017-01-10.	quagga	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3215
3305	CVE-2017-5486	HIGH	Critical	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3201
3306	CVE-2017-5485	HIGH	Critical	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in addrtoname.c:lookup_nsap().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3287
3307	CVE-2017-5484	HIGH	Critical	The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:sig_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3209
3308	CVE-2017-5483	HIGH	Critical	The SNMP parser in tcpdump before 4.9.0 has a buffer overflow in print-snmp.c:asn1_parse().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3289
3309	CVE-2017-5482	HIGH	Critical	The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2016-8575.	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3294
3310	CVE-2017-5473	MEDIUM	High	Cross-site request forgery (CSRF) vulnerability in ntopng through 2.4 allows remote attackers to hijack the authentication of arbitrary users, as demonstrated by admin/add_user.lua, admin/change_user_prefs.lua, admin/delete_user.lua, and admin/password_reset.lua.	ntop	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-5611
3311	CVE-2017-5462	MEDIUM	MEDIUM	A flaw in DRBG number generation within the Network Security Services (NSS) library where the internal state V does not correctly carry bits over. The NSS library has been updated to fix this issue to address this issue and Firefox ESR 52.1 has been updated with NSS version 3.28.4. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4107
3312	CVE-2017-5461	HIGH	Critical	Mozilla Network Security Services (NSS) before 3.21.4, 3.22.x through 3.28.x before 3.28.4, 3.29.x before 3.29.5, and 3.30.x before 3.30.1 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by leveraging incorrect base64 operations.	nss	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4232
3313	CVE-2017-5357	MEDIUM	High	regex.c in GNU ed before 1.14.1 allows attackers to cause a denial of service (crash) via a malformed command, which triggers an invalid free.	ed	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3431

	A	B	C	D	E	F	G	H	I	J	K	L	M
3314	CVE-2017-5356	MEDIUM	High	Irssi before 0.8.21 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a string containing a formatting sequence (%[) without a closing bracket ([).	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3557
3315	CVE-2017-5342	HIGH	Critical	In tcpdump before 4.9.0, a bug in multiple protocol parsers (Geneve, GRE, NSH, OTV, VXLAN and VXLAN GPE) could cause a buffer overflow in print-ether.c:ether_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3247
3316	CVE-2017-5341	HIGH	Critical	The OTV parser in tcpdump before 4.9.0 has a buffer overflow in print-otv.c:otv_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3203
3317	CVE-2017-5340	HIGH	Critical	Zend/zend_hash.c in PHP before 7.0.15 and 7.1.x before 7.1.1 mishandles certain cases that require large array allocations, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow, uninitialized memory access, and use of arbitrary destructor function pointers) via crafted serialized data.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2979
3318	CVE-2017-5337	HIGH	Critical	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to have unspecified impact via a crafted OpenPGP certificate.	gnutls	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3708
3319	CVE-2017-5336	HIGH	Critical	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.	gnutls	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3652
3320	CVE-2017-5335	MEDIUM	High	The stream reading functions in lib/opencdk/read-packet.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to cause a denial of service (out-of-memory error and crash) via a crafted OpenPGP certificate.	gnutls	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3792
3321	CVE-2017-5334	HIGH	Critical	Double free vulnerability in the gnutls_x509_ext_import_proxy function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via crafted policy language information in an X.509 certificate with a Proxy Certificate Information extension.	gnutls	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3649
3322	CVE-2017-5225	HIGH	Critical	LibTIFF version 4.0.7 is vulnerable to a heap buffer overflow in the tools/tiffcp resulting in DoS or code execution via a crafted BitsPerSample value.	libtiff	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3083
3323	CVE-2017-5209	MEDIUM	Critical	The base64decode function in base64.c in libimobiledevice libplist through 1.12 allows attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read) via split encoded Apple Property List data.	libplist	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3088
3324	CVE-2017-5205	HIGH	Critical	The ISAKMP parser in tcpdump before 4.9.0 has a buffer overflow in print-isakmp.c:ikev2_e_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3288
3325	CVE-2017-5204	HIGH	Critical	The IPv6 parser in tcpdump before 4.9.0 has a buffer overflow in print-ip6.c:ip6_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3280
3326	CVE-2017-5203	HIGH	Critical	The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3299
3327	CVE-2017-5202	HIGH	Critical	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3291
3328	CVE-2017-5196	MEDIUM	High	Irssi 0.8.18 before 0.8.21 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via vectors involving strings that are not UTF8.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3529
3329	CVE-2017-5195	MEDIUM	High	Irssi 0.8.17 before 0.8.21 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted ANSI x8 color code.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3573
3330	CVE-2017-5194	MEDIUM	High	Use-after-free vulnerability in Irssi before 0.8.21 allows remote attackers to cause a denial of service (crash) via an invalid nick message.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3578
3331	CVE-2017-5193	MEDIUM	High	The nickcmp function in Irssi before 0.8.21 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a message without a nick.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3498
3332	CVE-2017-5130	MEDIUM	High	An integer overflow in xmlmemory.c in libxml2 before 2.9.5, as used in Google Chrome prior to 62.0.3202.62 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted XML file.	libxml2	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3312
3333	CVE-2017-5123			A flaw was found in the upstream version of the kernels implementation of waitid systemcall. This flaw was the removal of validation of the target location where the kernel would copy the results. Previously it would implement a check to restrict the results to be copied to a valid userspace address, a new patch had inadvertently allowed copying to kernel addresses. An attacker could use this flaw to corrupt memory, panic the machine or possibly allow for arbitary memory writes.	linux	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4205
3334	CVE-2017-5029	MEDIUM	High	The xsltAddTextString function in transform.c in libxslt 1.1.29, as used in Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android, lacked a check for integer overflow during a size calculation, which allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.	libxslt	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4045

	A	B	C	D	E	F	G	H	I	J	K	L	M
3335	CVE-2017-3738	MEDIUM	Medium	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.	openssl	Unchanged	8.0.0.24	9.0.0.14	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2713
3336	CVE-2017-3737	MEDIUM	Medium	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an error state mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.	openssl	Unchanged	8.0.0.24	9.0.0.14	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2712
3337	CVE-2017-3736	MEDIUM	Medium	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.	openssl	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2475
3338	CVE-2017-3735	MEDIUM	High	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL since then.	openssl	Unchanged	8.0.0.22	9.0.0.11	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5186
3339	CVE-2017-3733	MEDIUM	High	During a renegotiation handshake if the Encrypt-Then-Mac (ETM) extension is negotiated where it was not in the original handshake (or vice-versa) then this can cause OpenSSL to crash (dependant on ciphersuite). Both clients and servers are affected.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3590
3340	CVE-2017-3732	MEDIUM	Medium	There is a carry propagating bug in the x86_64 Montgomery squaring procedure. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. For example this can occur by default in OpenSSL DHE based SSL/TLS ciphersuites.	openssl	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3128
3341	CVE-2017-3731	MEDIUM	High	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash.	openssl	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3127
3342	CVE-2017-3730	MEDIUM	High	If a malicious server supplies bad parameters for a DHE or ECDHE key exchange then this can result in the client attempting to dereference a NULL pointer leading to a client crash. This could be exploited in a Denial of Service Attack. resulting in a crash.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3129

	A	B	C	D	E	F	G	H	I	J	K	L	M
3343	CVE-2017-3653	LOW	Low	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4958
3344	CVE-2017-3652	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).	mysql	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4933
3345	CVE-2017-3651	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4942
3346	CVE-2017-3650	MEDIUM	Low	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: C API). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4927
3347	CVE-2017-3649	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5031
3348	CVE-2017-3648	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5056
3349	CVE-2017-3647	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4957
3350	CVE-2017-3646	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: X Plugin). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5006

	A	B	C	D	E	F	G	H	I	J	K	L	M
3351	CVE-2017-3645	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5076
3352	CVE-2017-3644	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4992
3353	CVE-2017-3643	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5090
3354	CVE-2017-3642	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5030
3355	CVE-2017-3641	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5041
3356	CVE-2017-3640	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5077
3357	CVE-2017-3639	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5039
3358	CVE-2017-3638	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4966

	A	B	C	D	E	F	G	H	I	J	K	L	M
3359	CVE-2017-3637	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: X Plugin). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4941
3360	CVE-2017-3636	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.56 and earlier and 5.6.36 and earlier. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	mysql	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4939
3361	CVE-2017-3635	LOW	Medium	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/C). Supported versions that are affected are 6.1.10 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. Note: The documentation has also been updated for the correct way to use mysql_stmt_close(). Please see: https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-execute.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-fetch.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-close.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-error.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-errno.html, and https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-sqlstate.html. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4977
3362	CVE-2017-3634	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5086
3363	CVE-2017-3633	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Memcached to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4935
3364	CVE-2017-3600	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. Note: CVE-2017-3600 is equivalent to CVE-2016-5483. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4083
3365	CVE-2017-3599	HIGH	High	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4086

	A	B	C	D	E	F	G	H	I	J	K	L	M
3366	CVE-2017-3589	LOW	Low	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 5.1.41 and earlier. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Connectors executes to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data. CVSS 3.0 Base Score 3.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4116
3367	CVE-2017-3586	MEDIUM	Medium	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 5.1.41 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. While the vulnerability is in MySQL Connectors, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.0 Base Score 6.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4065
3368	CVE-2017-3544	MEDIUM	Low	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SMTP to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	jdk&jre	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4016
3369	CVE-2017-3539	LOW	Low	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	jdk&jre	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4090
3370	CVE-2017-3533	MEDIUM	Low	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via FTP to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	jdk&jre	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4129
3371	CVE-2017-3529	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: UDF). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4988

	A	B	C	D	E	F	G	H	I	J	K	L	M
3372	CVE-2017-3526	HIGH	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4112
3373	CVE-2017-3523	MEDIUM	High	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J). Supported versions that are affected are 5.1.40 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. While the vulnerability is in MySQL Connectors, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4025
3374	CVE-2017-3514	MEDIUM	High	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4028
3375	CVE-2017-3512	MEDIUM	High	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 7u131 and 8u121. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4134
3376	CVE-2017-3511	LOW	High	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, Java SE Embedded, JRockit executes to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4087

	A	B	C	D	E	F	G	H	I	J	K	L	M
3377	CVE-2017-3509	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).	jdk&jre	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4143
3378	CVE-2017-3468	LOW	Low	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.7.17 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4126
3379	CVE-2017-3467	MEDIUM	Low	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: C API). Supported versions that are affected are 5.7.17 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4091
3380	CVE-2017-3465	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4135
3381	CVE-2017-3464	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4085
3382	CVE-2017-3463	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4058
3383	CVE-2017-3462	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4104

	A	B	C	D	E	F	G	H	I	J	K	L	M
3384	CVE-2017-3461	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4057
3385	CVE-2017-3460	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.17 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4149
3386	CVE-2017-3459	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.17 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4108
3387	CVE-2017-3458	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.17 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4088
3388	CVE-2017-3457	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.17 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4009
3389	CVE-2017-3456	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4132
3390	CVE-2017-3455	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4102
3391	CVE-2017-3454	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.17 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4023

	A	B	C	D	E	F	G	H	I	J	K	L	M
3392	CVE-2017-3453	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4110
3393	CVE-2017-3452	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.35 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4074
3394	CVE-2017-3450	MEDIUM	High	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4064
3395	CVE-2017-3331	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). The supported version that is affected is 5.7.11 to 5.7.17. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4019
3396	CVE-2017-3329	MEDIUM	High	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Thread Pooling). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4060
3397	CVE-2017-3320	LOW	Low	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS v3.0 Base Score 2.4 (Confidentiality impacts).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3269
3398	CVE-2017-3319	LOW	Low	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: X Plugin). Supported versions that are affected are 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS v3.0 Base Score 3.1 (Confidentiality impacts).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3311
3399	CVE-2017-3318	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Error Handling). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.0 (Confidentiality impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3319

	A	B	C	D	E	F	G	H	I	J	K	L	M
3400	CVE-2017-3317	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Logging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.0 (Availability impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3271
3401	CVE-2017-3313	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: MyISAM). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.7 (Confidentiality impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3258
3402	CVE-2017-3312	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.7 (Confidentiality, Integrity and Availability impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3218
3403	CVE-2017-3309	MEDIUM	High	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4148
3404	CVE-2017-3308	MEDIUM	High	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4111
3405	CVE-2017-3305	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: C API). Supported versions that are affected are 5.5.54 and earlier and 5.6.35 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).	mysql	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4103
3406	CVE-2017-3304	MEDIUM	Medium	Vulnerability in the MySQL Cluster component of Oracle MySQL (subcomponent: Cluster: DD). Supported versions that are affected are 7.2.27 and earlier, 7.3.16 and earlier, 7.4.14 and earlier and 7.5.5 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4114
3407	CVE-2017-3291	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3194

	A	B	C	D	E	F	G	H	I	J	K	L	M
3408	CVE-2017-3289	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts).	jdk&jre	Unchanged	8.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3178
3409	CVE-2017-3273	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3274
3410	CVE-2017-3272	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3165
3411	CVE-2017-3265	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 5.6 (Confidentiality and Availability impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3314
3412	CVE-2017-3262	MEDIUM	Medium	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Java Mission Control). The supported version that is affected is Java SE: 8u112. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: Applies to Java Mission Control Installation. CVSS v3.0 Base Score 5.3 (Confidentiality impacts).	jdk&jre	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3181
3413	CVE-2017-3261	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 4.3 (Confidentiality impacts).	jdk&jre	Unchanged	8.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3211

	A	B	C	D	E	F	G	H	I	J	K	L	M
3414	CVE-2017-3260	MEDIUM	High	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 7u121 and 8u112. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts).	jdk&jre	Unchanged	8.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3160
3415	CVE-2017-3259	MEDIUM	Low	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 3.7 (Confidentiality impacts).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3309
3416	CVE-2017-3258	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3283
3417	CVE-2017-3257	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.6.34 and earlier5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3241
3418	CVE-2017-3256	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3284
3419	CVE-2017-3253	MEDIUM	High	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS v3.0 Base Score 7.5 (Availability impacts).	jdk&jre	Unchanged	8.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3290

	A	B	C	D	E	F	G	H	I	J	K	L	M
3420	CVE-2017-3252	LOW	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAAS). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS v3.0 Base Score 5.8 (Integrity impacts).	jdk&jre	Unchanged	8.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3177
3421	CVE-2017-3251	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.9 (Availability impacts).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3270
3422	CVE-2017-3244	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3191
3423	CVE-2017-3243	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.53 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.4 (Availability impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3193
3424	CVE-2017-3241	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS v3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3318
3425	CVE-2017-3238	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).	mysql	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3190
3426	CVE-2017-3231	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 4.3 (Confidentiality impacts).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3159

	A	B	C	D	E	F	G	H	I	J	K	L	M
3427	CVE-2017-3226	MEDIUM	MEDIUM	Das U-Boot is a device bootloader that can read its configuration from an AES encrypted file. Devices that make use of Das U-Boot's AES-CBC encryption feature using environment encryption (i.e., setting the configuration parameter CONFIG_ENV_AES=y) read environment variables from disk as the encrypted disk image is processed. An attacker with physical access to the device can manipulate the encrypted environment data to include a crafted two-byte sequence which triggers an error in environment variable parsing. This error condition is improperly handled by Das U-Boot, resulting in an immediate process termination with a debugging message.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4395
3428	CVE-2017-3225	LOW	MEDIUM	Das U-Boot is a device bootloader that can read its configuration from an AES encrypted file. For devices utilizing this environment encryption mode, U-Boot's use of a zero initialization vector may allow attacks against the underlying cryptographic implementation and allow an attacker to decrypt the data. Das U-Boot's AES-CBC encryption feature uses a zero (0) initialization vector. This allows an attacker to perform dictionary attacks on encrypted data produced by Das U-Boot to learn information about the encrypted data.	u-boot	Unchanged	Won't Fix	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4430
3429	CVE-2017-3224	MEDIUM	HIGH	Open Shortest Path First (OSPF) protocol implementations may improperly determine Link State Advertisement (LSA) recency for LSAs with MaxSequenceNumber. According to RFC 2328 section 13.1, for two instances of the same LSA, recency is determined by first comparing sequence numbers, then checksums, and finally MaxAge. In a case where the sequence numbers are the same, the LSA with the larger checksum is considered more recent, and will not be flushed from the Link State Database (LSDB). Since the RFC does not explicitly state that the values of links carried by a LSA must be the same when prematurely aging a self-originating LSA with MaxSequenceNumber, it is possible in vulnerable OSPF implementations for an attacker to craft a LSA with MaxSequenceNumber and invalid links that will result in a larger checksum and thus a 'newer' LSA that will not be flushed from the LSDB. Propagation of the crafted LSA can result in the erasure or alteration of the routing tables of routers within the routing domain, creating a denial of service condition or the re-routing of traffic on the the network. CVE-2017-3224 has been reserved for Quagga and downstream implementations (SUSE, openSUSE, and Red Hat packages).	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4376
3430	CVE-2017-3169	HIGH	Critical	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.	apache2	Unchanged	8.0.0.20	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4541
3431	CVE-2017-3167	HIGH	Critical	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.	apache2	Unchanged	8.0.0.20	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4540
3432	CVE-2017-3145	MEDIUM	HIGH	Improper sequencing during cleanup operations of upstream recursion fetch contexts in BIND can lead to a use-after-free error, triggering an assertion failure and crash in named.	bind	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4445
3433	CVE-2017-3144	MEDIUM	HIGH	It was found that omapi code doesn't free socket descriptor if empty message was sent by client, which allows malicious client to use up all available descriptors causing Denial of Service	dhcp	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3198
3434	CVE-2017-3143	MEDIUM	MEDIUM	A flaw was found in the way BIND handled TSIG authentication for dynamic updates. A remote attacker able to communicate with an authoritative BIND server could use this flaw to manipulate the contents of a zone, by forging a valid TSIG or SIG(0) signature for a dynamic update request.	bind	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4662
3435	CVE-2017-3142	MEDIUM	LOW	A flaw was found in the way BIND handled TSIG authentication of AXFR requests. A remote attacker, able to communicate with an authoritative BIND server, could use this flaw to view the entire contents of a zone by sending a specially constructed request packet.	bind	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4675
3436	CVE-2017-3141	HIGH	HIGH	The BIND installer on Windows uses an unquoted service path which can enable a local user to achieve privilege escalation if the host file system permissions allow this.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4535
3437	CVE-2017-3140	MEDIUM	MEDIUM	If named is configured to use Response Policy Zones (RPZ) an error processing some rule types can lead to a condition where BIND will endlessly loop while handling a query.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4515
3438	CVE-2017-3139	Medium	HIGH	A denial of service flaw was found in the way BIND handled DNSSEC validation. A remote attacker could use this flaw to make named exit unexpectedly with an assertion failure via a specially crafted DNS response.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3889
3439	CVE-2017-3138	LOW	MEDIUM	A denial of service flaw was found in the way BIND processed control channel commands. A remote attacker with access to the BIND control channel could use this flaw to make named exit unexpectedly with an assertion failure via a specially crafted command.	bind	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4081
3440	CVE-2017-3137	MEDIUM	HIGH	A denial of service flaw was found in the way BIND handled a query response containing CNAME or DNAME resource records in an unusual order. A remote attacker could use this flaw to make named exit unexpectedly with an assertion failure via a specially crafted DNS response. unexpectedly with an assertion failure via a specially crafted command.	bind	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4136

	A	B	C	D	E	F	G	H	I	J	K	L	M
3441	CVE-2017-3136	MEDIUM	MEDIUM	A denial of service flaw was found in the way BIND handled query requests when using DNS64 with "break-dnssec yes" option. A remote attacker could use this flaw to make named exit unexpectedly with an assertion failure via a specially crafted DNS request. unexpectedly with an assertion failure via a specially crafted command.	bind	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4120
3442	CVE-2017-3135	MEDIUM	MEDIUM	Under some conditions when using both DNS64 and RPZ to rewrite query responses, query processing can resume in an inconsistent state leading to either an INSIST assertion failure or an attempt to read through a NULL pointer.	bind	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3164
3443	CVE-2017-2888	MEDIUM	High	An exploitable integer overflow vulnerability exists when creating a new RGB Surface in SDL 2.0.5. A specially crafted file can cause an integer overflow resulting in too little memory being allocated which can lead to a buffer overflow and potential code execution. An attacker can provide a specially crafted image file to trigger this vulnerability.	sdl	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5554
3444	CVE-2017-2887	MEDIUM	High	An exploitable buffer overflow vulnerability exists in the XCF property handling functionality of SDL_image 2.0.1. A specially crafted xcf file can cause a stack-based buffer overflow resulting in potential code execution. An attacker can provide a specially crafted XCF file to trigger this vulnerability.	libsdl2-image	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5585
3445	CVE-2017-2885	HIGH	CRITICAL	An exploitable stack based buffer overflow vulnerability exists in the GNOME libsoup 2.58. A specially crafted HTTP request can cause a stack overflow resulting in remote code execution. An attacker can send a special HTTP request to the vulnerable server to trigger this vulnerability.	libsoup	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3869
3446	CVE-2017-2870	Medium	High	An exploitable integer overflow vulnerability exists in the tiff_image_parse functionality of Gdk-Pixbuf 2.36.6 when compiled with Clang. A specially crafted tiff file can cause a heap-overflow resulting in remote code execution. An attacker can send a file or a URL to trigger this vulnerability.	gdk-pixbuf	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5222
3447	CVE-2017-2862	Medium	High	An exploitable heap overflow vulnerability exists in the gdk_pixbuf__jpeg_image_load_incrementf functionality of Gdk-Pixbuf 2.36.6. A specially crafted jpeg file can cause a heap overflow resulting in remote code execution. An attacker can send a file or url to trigger this vulnerability.	gdk-pixbuf	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5250
3448	CVE-2017-2825	MEDIUM	HIGH	In the trapper functionality of Zabbix Server 2.4.x, specifically crafted trapper packets can pass database logic checks, resulting in database writes. An attacker can set up a Man-in-the-Middle server to alter trapper requests made between an active Zabbix proxy and Server to trigger this vulnerability.	zabbix	Unchanged	Won't Fix	Vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3803
3449	CVE-2017-2820	MEDIUM	High	An exploitable integer overflow vulnerability exists in the JPEG 2000 image parsing functionality of freedesktop.org Poppler 0.53.0. A specially crafted PDF file can lead to an integer overflow causing out of bounds memory overwrite on the heap resulting in potential arbitrary code execution. To trigger this vulnerability, a victim must open the malicious PDF in an application using this library.	poppler	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4655
3450	CVE-2017-2818	MEDIUM	High	An exploitable heap overflow vulnerability exists in the image rendering functionality of Poppler 0.53.0. A specifically crafted PDF can cause an overly large number of color components during image rendering, resulting in heap corruption. An attacker controlled PDF file can be used to trigger this vulnerability.	poppler	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4644
3451	CVE-2017-2814	MEDIUM	High	An exploitable heap overflow vulnerability exists in the image rendering functionality of Poppler 0.53.0. A specifically crafted pdf can cause an image resizing after allocation has already occurred, resulting in heap corruption which can lead to code execution. An attacker controlled PDF file can be used to trigger this vulnerability.	poppler	Unchanged	Won't Fix	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4663
3452	CVE-2017-2671	MEDIUM	Medium	The ping_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which allows local users to cause a denial of service (panic) by leveraging access to the protocol value of IPPROTO_ICMP in a socket system call.	linux	Unchanged	8.0.0.17	9.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3973
3453	CVE-2017-2669	MEDIUM	HIGH	Dovecot before version 2.2.29 is vulnerable to a denial of service. When 'dict' passdb and userdb were used for user authentication, the username sent by the IMAP/POP3 client was sent through var_expand() to perform %variable expansion. Sending specially crafted %variable fields could result in excessive memory usage causing the process to crash (and restart), or excessive CPU usage causing all authentications to hang.	dovecot	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4219
3454	CVE-2017-2659	Medium	HIGH	It was found that dropbear before version 2013.59 with GSSAPI leaks whether given username is valid or invalid. When an invalid username is given, the GSSAPI authentication failure was incorrectly counted towards the maximum allowed number of password attempts.	dropbear	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3752
3455	CVE-2017-2647	HIGH	High	The KEYS subsystem in the Linux kernel before 3.18 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via vectors involving a NULL value for a certain match field, related to the keyring_search_iterator function in keyring.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3946
3456	CVE-2017-2640	HIGH	CRITICAL	An out-of-bounds write flaw was found in the way Pidgin before 2.12.0 processed XML content. A malicious remote server could potentially use this flaw to crash Pidgin or execute arbitrary code in the context of the pidgin process.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4433
3457	CVE-2017-2636	HIGH	High	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.	linux	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3516

	A	B	C	D	E	F	G	H	I	J	K	L	M
3458	CVE-2017-2635	MEDIUM	MEDIUM	A NULL pointer dereference vulnerability was found in virStorageSourceUpdateBlockPhysicalSize when attempted to call on empty drives. Unprivileged local user can trigger this bug to crash libvirtd.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4368
3459	CVE-2017-2634	HIGH	HIGH	A flaw was found in the linux kernels implementation of DCCP protocol in which a an application making a DCCP connection over IPV6 could crash a remote (or local) system. When attempting to send a DCCP reset packet, the system will incorrectly create the packet header and while updating the SNMP counters for this condition crash the kernel. The remote system would need to have both an application running as a DCCP server and have an IPV6 address routable.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4275
3460	CVE-2017-2633	MEDIUM	MEDIUM	Quick Emulator(Qemu) built with the VNC display driver support is vulnerable to an out-of-bounds memory access issue. It could occur while refreshing the vnc display surface area in 'vnc_refresh_server_surface'	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4287
3461	CVE-2017-2630	MEDIUM	HIGH	Quick Emulator(Qemu) built with the Network Block Device(NBD) client support is vulnerable to a stack buffer overflow issue. It could occur while processing server's response to a 'NBD_OPT_LIST' request.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4212
3462	CVE-2017-2629	MEDIUM	MEDIUM	A coding mistake was found in TLS Certificate Status Request extension feature that asks for a fresh proof of the server's certificate's validity in the code that checks for a test success or failure. It ends up always thinking there's valid proof, even when there is none or if the server doesn't support the TLS extension in question. Contrary to how it used to function and contrary to how this feature is documented to work.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3388
3463	CVE-2017-2626	LOW	MEDIUM	It was discovered that libICE before 1.0.9-8 used a weak entropy to generate keys. A local attacker could potentially use this flaw for session hijacking using the information available from the process list.	libice	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-4457
3464	CVE-2017-2625	LOW	MEDIUM	It was discovered that libXdmcp before 1.1.2 including used weak entropy to generate session keys. On a multi-user system using xdmcp, a local attacker could potentially use information available from the process list to brute force the key, allowing them to hijack other users' sessions.	libxdmcp	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4398
3465	CVE-2017-2624	LOW	HIGH	It was found that xorg-x11-server before 1.19.0 including uses memcmp() to check the received MIT cookie against a series of valid cookies. If the cookie is correct, it is allowed to attach to the Xorg session. Since most memcmp() implementations return after an invalid byte is seen, this causes a time difference between a valid and invalid byte, which could allow an efficient brute force attack.	xserver-xorg	Unchanged	8.0.0.27	9.0.0.18	Not vulnerable	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4438
3466	CVE-2017-2620	HIGH	CRITICAL	Quick emulator(Qemu) built with the Cirrus CLGD 54xx VGA Emulator support is vulnerable to an out-of-bounds access issue. It could occur while copying VGA data in cirrus_bitblt_cputovideo.	qemu	Unchanged	8.0.0.27	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4199
3467	CVE-2017-2619	MEDIUM	HIGH	Samba before versions 4.6.1, 4.5.7 and 4.4.11 are vulnerable to a malicious client using a symlink race to allow access to areas of the server file system not exported under the share definition.	samba	Unchanged	Vulnerable	9.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3505
3468	CVE-2017-2618	MEDIUM	MEDIUM	A flaw was found in the Linux kernels handling of clearing SELinux attributes on /proc/pid/attr files. An empty (null) write to this file can crash the system by causing the system to attempt to access unmapped kernel memory.	linux	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4182
3469	CVE-2017-2616	MEDIUM	MEDIUM	A race condition was found in util-linux before 2.32.1 in the way su handled the management of child processes. A local authenticated attacker could use this flaw to kill other processes with root privileges under specific conditions.	util-linux	Unchanged	8.0.0.27	9.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4369
3470	CVE-2017-2615	HIGH	CRITICAL	Quick emulator(Qemu) built with the Cirrus CLGD 54xx VGA Emulator support is vulnerable to an out-of-bounds access issue. It could occur while copying VGA data via bitblt copy in backward mode.	qemu	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3389
3471	CVE-2017-2596	MEDIUM	Medium	The nested_vmx_check_vmptr function in arch/x86/kvm/vmx.c in the Linux kernel through 4.9.8 improperly emulates the VMXON instruction, which allows KVM L1 guest OS users to cause a denial of service (host OS memory consumption) by leveraging the mishandling of page references.	linux	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3187
3472	CVE-2017-2595	MEDIUM	MEDIUM	It was found that the log file viewer in Red Hat JBoss Enterprise Application 6 and 7 allows arbitrary file read to authenticated user via path traversal.	wildfly	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-9517
3473	CVE-2017-2592	LOW	MEDIUM	python-oslo-middleware before versions 3.8.1, 3.19.1, 3.23.1 is vulnerable to an information disclosure. Software using the CatchError class could include sensitive values in a traceback's error message. System users could exploit this flaw to obtain sensitive information from OpenStack component error logs (for example, keystone tokens).	python-oslo-middleware	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3920
3474	CVE-2017-2584	LOW	High	arch/x86/kvm/emulate.c in the Linux kernel through 4.9.3 allows local users to obtain sensitive information from kernel memory or cause a denial of service (use-after-free) via a crafted application that leverages instruction emulation for fxrstor, fxsave, sgdt, and sidt.	linux	Unchanged	8.0.0.15	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3079
3475	CVE-2017-2583	MEDIUM	High	The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 improperly emulates a MOV SS, NULL selector instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gain guest OS privileges via a crafted application.	linux	Unchanged	8.0.0.15	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3197
3476	CVE-2017-18641	HIGH	HIGH	In LXC 2.0, many template scripts download code over cleartext HTTP, and omit a digital-signature check, before running it to bootstrap containers.	lxc	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-4042

	A	B	C	D	E	F	G	H	I	J	K	L	M
3477	CVE-2017-18635	Medium	MEDIUM	An XSS vulnerability was discovered in noVNC before 0.6.2 in which the remote VNC server could inject arbitrary HTML into the noVNC web page via the messages propagated to the status field, such as the VNC server name.	novnc	Unchanged	Investigate	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4979
3478	CVE-2017-18595	High	HIGH	An issue was discovered in the Linux kernel before 4.14.11. A double free may be caused by the function allocate_trace_buffer in the file kernel/trace/trace.c.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4839
3479	CVE-2017-18594	MEDIUM	HIGH	nse_libssh2.cc in Nmap 7.70 is subject to a denial of service condition due to a double free when an SSH connection fails, as demonstrated by a leading \n character to ssh-brute.nse or ssh-auth-methods.nse.	nmap	Unchanged	Not vulnerable	Not vulnerable	10.17.41.18	10.18.44.11	Not vulnerable	Not vulnerable	LIN1018-4806
3480	CVE-2017-18552	Medium	HIGH	An issue was discovered in net/rds/af_rds.c in the Linux kernel before 4.11. There is an out of bounds write and read in the function rds_recv_track_latency.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4713
3481	CVE-2017-18551	Medium	HIGH	An issue was discovered in drivers/i2c/i2c-core-smbus.c in the Linux kernel before 4.14.15. There is an out of bounds write in the function i2c_smbus_xfer_emulated.	linux	Unchanged	8.0.0.31	9.0.0.24	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4711
3482	CVE-2017-18550	Low	MEDIUM	An issue was discovered in drivers/scsi/aacraid/commctrl.c in the Linux kernel before 4.13. There is potential exposure of kernel stack memory because aac_get_hba_info does not initialize the hbainfo structure.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4710
3483	CVE-2017-18549	Low	MEDIUM	An issue was discovered in drivers/scsi/aacraid/commctrl.c in the Linux kernel before 4.13. There is potential exposure of kernel stack memory because aac_send_raw_srb does not initialize the reply structure.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.19	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4709
3484	CVE-2017-18509	High	HIGH	An issue was discovered in net/ipv6/ip6mr.c in the Linux kernel before 4.11. By setting a specific socket option, an attacker can control a pointer in kernel land and cause an inet_csk_listen_stop general protection fault, or potentially execute arbitrary code under certain circumstances. The issue can be triggered as root (e.g., inside a default LXC container or with the CAP_NET_ADMIN capability) or after namespace unsharing. This occurs because sk_type and protocol are not checked in the appropriate part of the ip6_mroute_* functions. NOTE: this affects Linux distributions that use 4.9.x longterm kernels before 4.9.187.	linux	Unchanged	8.0.0.31	9.0.0.24	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4660
3485	CVE-2017-18379	HIGH	CRITICAL	In the Linux kernel before 4.14, an out of boundary access happened in drivers/nvme/target/fc.c.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.18	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4545
3486	CVE-2017-18360	Medium	MEDIUM	In change_port_settings in drivers/usb/serial/io_ti.c in the Linux kernel before 4.11.3, local users could cause a denial of service by division-by-zero in the serial device layer by trying to set very high baud rates.	linux	Unchanged	8.0.0.30	9.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3529
3487	CVE-2017-18344	LOW	MEDIUM	The timer_create syscall implementation in kernel/time/posix-timers.c in the Linux kernel before 4.14.8 doesn't properly validate the sigevent->sigev_notify field, which leads to out-of-bounds access in the show_timer function (called when /proc/$PID/timers is read). This allows userspace applications to read arbitrary kernel memory (on a kernel built with CONFIG_POSIX_TIMERS and CONFIG_CHECKPOINT_RESTORE).	linux	Unchanged	8.0.0.27	9.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4450
3488	CVE-2017-18342	HIGH	CRITICAL	In PyYAML before 4.1, the yaml.load() API could execute arbitrary code. In other words, yaml.safe_load is not used.	python-pyyaml	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4220
3489	CVE-2017-18273	HIGH	MEDIUM	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22, an infinite loop vulnerability was found in the function ReadTXTImage in coders/txt.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted image file that is mishandled in a GetImageIndexInList call.	imagemagick	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4029
3490	CVE-2017-18272	MEDIUM	MEDIUM	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-25, there is a use-after-free in ReadOneMNGImage in coders/png.c, which allows attackers to cause a denial of service via a crafted MNG image file that is mishandled in an MngInfoDiscardObject call.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4034
3491	CVE-2017-18271	HIGH	MEDIUM	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22, an infinite loop vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted MIFF image file.	imagemagick	Unchanged	8.0.0.27	9.0.0.17	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4056
3492	CVE-2017-18270	LOW	HIGH	In the Linux kernel before 4.13.5, a local user could create keyrings for other users via keyctl commands, setting unwanted defaults or causing a denial of service.	linux	Unchanged	8.0.0.30	9.0.0.20	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4051
3493	CVE-2017-18269	HIGH	CRITICAL	An SSE2-optimized memmove implementation for i386 in sysdeps/i386/i686/multiarch/memcpy-sse2-unaligned.S in the GNU C Library (aka glibc or libc6) 2.21 through 2.27 does not correctly perform the overlapping memory check if the source memory range spans the middle of the address space, resulting in corrupt data being produced by the copy operation. This may disclose information to context-dependent attackers, or result in a denial of service, or, possibly, code execution.	glibc	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4036
3494	CVE-2017-18267	MEDIUM	MEDIUM	The FoFiType1C::cvtGlyph function in fofi/FoFiType1C.cc in Poppler through 0.64.0 allows remote attackers to cause a denial of service (infinite recursion) via a crafted PDF file, as demonstrated by pdftops.	poppler	Unchanged	Won't Fix	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3921
3495	CVE-2017-18266	MEDIUM	HIGH	The open_envvar function in xdg-open in xdg-utils before 1.1.3 does not validate strings before launching the program specified by the BROWSER environment variable, which might allow remote attackers to conduct argument-injection attacks via a crafted URL, as demonstrated by %s in this environment variable.	xdg-utils	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3938

	A	B	C	D	E	F	G	H	I	J	K	L	M
3496	CVE-2017-18264	HIGH	CRITICAL	An issue was discovered in libraries/common.inc.php in phpMyAdmin 4.0 before 4.0.10.20, 4.4.x, 4.6.x, and 4.7.0 prereleases. The restrictions caused by $cfg['Servers'][$i] ['AllowNoPassword'] = false are bypassed under certain PHP versions (e.g., version 5). This can allow the login of users who have no password set even if the administrator has set $cfg['Servers'] [$i]['AllowNoPassword'] to false (which is also the default). This occurs because some implementations of the PHP substr function return false when given '' as the first argument.	phpmyadmin	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3927
3497	CVE-2017-18261	MEDIUM	MEDIUM	The arch_timer_reg_read_stable macro in arch/arm64/include/asm/arch_timer.h in the Linux kernel before 4.13 allows local users to cause a denial of service (infinite recursion) by writing to a file under /sys/kernel/debug in certain circumstances, as demonstrated by a scenario involving debugfs, ftrace, PREEMPT_TRACER, and FUNCTION_GRAPH_TRACER.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3846
3498	CVE-2017-18258	MEDIUM	MEDIUM	The xz_head function in xzlib.c in libxml2 before 2.9.6 allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file, because the decoder functionality does not restrict memory usage to what is required for a legitimate file.	libxml2	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3724
3499	CVE-2017-18257	MEDIUM	MEDIUM	The __get_data_block function in fs/f2fs/data.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow and loop) via crafted use of the open and fallocate system calls with an FS_IOC_FIEMAP ioctl.	linux	Unchanged	Not vulnerable	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3740
3500	CVE-2017-18255	MEDIUM	HIGH	The perf_cpu_time_max_percent_handler function in kernel/events/core.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow) or possibly have unspecified other impact via a large value, as demonstrated by an incorrect sample-rate calculation.	linux	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3657
3501	CVE-2017-18254	Medium	MEDIUM	An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function WriteGIFImage in coders/gif.c, which allow remote attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3649
3502	CVE-2017-18253	Medium	MEDIUM	An issue was discovered in ImageMagick 7.0.7. A NULL pointer dereference vulnerability was found in the function LoadOpenCLDevices in MagickCore/opencl.c, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	Not vulnerable	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3646
3503	CVE-2017-18252	Medium	MEDIUM	An issue was discovered in ImageMagick 7.0.7. The MogrifyImageList function in MagickWand/mogrify.c allows attackers to cause a denial of service (assertion failure and application exit in ReplaceImageInList) via a crafted file.	imagemagick	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3647
3504	CVE-2017-18251	Medium	MEDIUM	An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function ReadPCDImage in coders/pcd.c, which allow remote attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3648
3505	CVE-2017-18250	Medium	MEDIUM	An issue was discovered in ImageMagick 7.0.7. A NULL pointer dereference vulnerability was found in the function LogOpenCLBuildFailure in MagickCore/opencl.c, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	Not vulnerable	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3655
3506	CVE-2017-18249	MEDIUM	HIGH	The add_free_nid function in fs/f2fs/node.c in the Linux kernel before 4.12 does not properly track an allocated nid, which allows local users to cause a denial of service (race condition) or possibly have unspecified other impact via concurrent threads.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3663
3507	CVE-2017-18248	LOW	MEDIUM	The add_job function in scheduler/ipp.c in CUPS before 2.2.6, when D-Bus support is enabled, can be crashed by remote attackers by sending print jobs with an invalid username, related to a D-Bus notification.	cups	Unchanged	8.0.0.26	9.0.0.16	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3639
3508	CVE-2017-18247	MEDIUM	MEDIUM	The av_audio_fifo_size function in libavutil/audio_fifo.c in Libav 12.2 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted media file.	libav	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-3643
3509	CVE-2017-18246	MEDIUM	MEDIUM	The pcm_encode_frame function in libavcodec/pcm.c in Libav 12.2 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted media file.	libav	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3641
3510	CVE-2017-18245	MEDIUM	MEDIUM	The mpc8_probe function in libavformat/mpc8.c in Libav 12.2 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted audio file.	libav	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3675
3511	CVE-2017-18244	MEDIUM	MEDIUM	The stereo_processing function in libavcodec/aacps.c in Libav 12.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted aac file, related to ff_ps_apply.	libav	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3654
3512	CVE-2017-18243	MEDIUM	MEDIUM	The unpack_parse_unit function in libavcodec/dirac_parser.c in Libav 12.2 allows remote attackers to cause a denial of service (segmentation fault) via a crafted file.	libav	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3633
3513	CVE-2017-18242	MEDIUM	MEDIUM	The apply_dependent_coupling function in libavcodec/aacdec.c in Libav 12.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted aac file.	libav	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3669
3514	CVE-2017-18241	MEDIUM	MEDIUM	fs/f2fs/segment.c in the Linux kernel before 4.13 allows local users to cause a denial of service (NULL pointer dereference and panic) by using a noflush_merge option that triggers a NULL value for a flush_cmd_control data structure.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3666
3515	CVE-2017-18232	LOW	MEDIUM	The Serial Attached SCSI (SAS) implementation in the Linux kernel through 4.15.9 mishandles a mutex within libsas, which allows local users to cause a denial of service (deadlock) by triggering certain error-handling code.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3547

	A	B	C	D	E	F	G	H	I	J	K	L	M
3516	CVE-2017-18224	LOW	MEDIUM	In the Linux kernel before 4.15, fs/ocfs2/aops.c omits use of a semaphore and consequently has a race condition for access to the extent tree during read operations in DIRECT mode, which allows local users to cause a denial of service (BUG) by modifying a certain e_cpos field.	linux	Unchanged	Not vulnerable	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3510
3517	CVE-2017-18222	MEDIUM	HIGH	In the Linux kernel before 4.12, Hisilicon Network Subsystem (HNS) does not consider the ETH_SS_PRIV_FLAGS case when retrieving sset_count data, which allows local users to cause a denial of service (buffer overflow and memory corruption) or possibly have unspecified other impact, as demonstrated by incompatibility between hns_get_sset_count and ethtool_get_strings.	linux	Unchanged	Not vulnerable	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3539
3518	CVE-2017-18221	MEDIUM	MEDIUM	The __munlock_pagevec function in mm/mlock.c in the Linux kernel before 4.11.4 allows local users to cause a denial of service (NR_MLOCK accounting corruption) via crafted use of mlockall and munlockall system calls.	linux	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3542
3519	CVE-2017-18218	HIGH	HIGH	In drivers/net/ethernet/hisilicon/hns/hns_enet.c in the Linux kernel before 4.13, local users can cause a denial of service (use-after-free and BUG) or possibly have unspecified other impact by leveraging differences in skb handling between hns_nic_net_xmit_hw and hns_nic_net_xmit.	linux	Unchanged	Not vulnerable	9.0.0.17	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3567
3520	CVE-2017-18216	LOW	MEDIUM	In fs/ocfs2/cluster/nodemanager.c in the Linux kernel before 4.15, local users can cause a denial of service (NULL pointer dereference and BUG) because a required mutex is not used.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3535
3521	CVE-2017-18211	HIGH	CRITICAL	In ImageMagick 7.0.7, a NULL pointer dereference vulnerability was found in the function saveBinaryCLProgram in magick/opencl.c because a program-lookup result is not checked, related to CacheOpenCLKernel.	imagemagick	Unchanged	Not vulnerable	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3541
3522	CVE-2017-18210	HIGH	CRITICAL	In ImageMagick 7.0.7, a NULL pointer dereference vulnerability was found in the function BenchmarkOpenCLDevices in MagickCore/opencl.c because a memory allocation result is not checked.	imagemagick	Unchanged	Not vulnerable	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3519
3523	CVE-2017-18209	MEDIUM	HIGH	In the GetOpenCLCachedFilesDirectory function in magick/opencl.c in ImageMagick 7.0.7, a NULL pointer dereference vulnerability occurs because a memory allocation result is not checked, related to GetOpenCLCacheDirectory.	imagemagick	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3531
3524	CVE-2017-18208	MEDIUM	MEDIUM	The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause a denial of service (infinite loop) by triggering use of MADVISE_WILLNEED for a DAX mapping.	linux	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3516
3525	CVE-2017-18207	MEDIUM	MEDIUM	** DISPUTED ** The Wave_read._read_fmt_chunk function in Lib/wave.py in Python through 3.6.4 does not ensure a nonzero channel value, which allows attackers to cause a denial of service (divide-by-zero and exception) via a crafted wav format audio file. NOTE: the vendor disputes this issue because Python applications need to be prepared to handle a wide variety of exceptions.	python	Unchanged	Investigate	Investigate	10.17.41.19	10.18.44.14	Not vulnerable	Not vulnerable	LIN1019-3676
3526	CVE-2017-18206	HIGH	CRITICAL	In utils.c in zsh before 5.4, symlink expansion had a buffer overflow.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3552
3527	CVE-2017-18205	MEDIUM	HIGH	In builtin.c in zsh before 5.4, when sh compatibility mode is used, there is a NULL pointer dereference during processing of the cd command with no argument if HOME is not set.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3538
3528	CVE-2017-18204	LOW	MEDIUM	The ocfs2_setattr function in fs/ocfs2/file.c in the Linux kernel before 4.14.2 allows local users to cause a denial of service (deadlock) via DIO requests.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3536
3529	CVE-2017-18203	LOW	MEDIUM	The dm_get_from_kobject function in drivers/md/dm.c in the Linux kernel before 4.14.3 allow local users to cause a denial of service (BUG) by leveraging a race condition with __dm_destroy during creation and removal of DM devices.	linux	Unchanged	8.0.0.26	9.0.0.15	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3515
3530	CVE-2017-18202	HIGH	CRITICAL	The __oom_reap_task_mm function in mm/oom_kill.c in the Linux kernel before 4.14.4 mishandles gather operations, which allows attackers to cause a denial of service (TLB entry leak or use-after-free) or possibly have unspecified other impact by triggering a copy_to_user call within a certain time window.	linux	Unchanged	Not vulnerable	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3413
3531	CVE-2017-18201	HIGH	CRITICAL	An issue was discovered in GNU libcdio before 2.0.0. There is a double free in get_cdtext_generic() in lib/driver/_cdio_generic.c.	libcdio	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3403
3532	CVE-2017-18200	MEDIUM	MEDIUM	The f2fs implementation in the Linux kernel before 4.14 mishandles reference counts associated with f2fs_wait_discard_bios calls, which allows local users to cause a denial of service (BUG), as demonstrated by fstrim.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3362
3533	CVE-2017-18199	MEDIUM	MEDIUM	realloc_symlink in rock.c in GNU libcdio before 1.0.0 allows remote attackers to cause a denial of service (NULL Pointer Dereference) via a crafted iso file.	libcdio	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3426
3534	CVE-2017-18198	MEDIUM	HIGH	print_iso9660_recurse in iso-info.c in GNU libcdio before 1.0.0 allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted iso file.	libcdio	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3415
3535	CVE-2017-18196	LOW	LOW	Leptonica 1.74.4 constructs unintended pathnames (containing duplicated path components) when operating on files in /tmp subdirectories, which might allow local users to bypass intended file restrictions by leveraging access to a directory located deeper within the /tmp directory tree, as demonstrated by /tmp/ANY/PATH/ANY/PATH/input.tif.	leptonica	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3422
3536	CVE-2017-18193	MEDIUM	Medium	fs/f2fs/extent_cache.c in the Linux kernel before 4.13 mishandles extent trees, which allows local users to cause a denial of service (BUG) via an application with multiple threads.	linux	Unchanged	Vulnerable	9.0.0.15	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3379

	A	B	C	D	E	F	G	H	I	J	K	L	M
3537	CVE-2017-18190	MEDIUM	HIGH	A localhost.localdomain whitelist entry in valid_host() in scheduler/client.c in CUPS before 2.2.2 allows remote attackers to execute arbitrary IPP commands by sending POST requests to the CUPS daemon in conjunction with DNS rebinding. The localhost.localdomain name is often resolved via a DNS server (neither the OS nor the web browser is responsible for ensuring that localhost.localdomain is 127.0.0.1).	cups	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3338
3538	CVE-2017-18189	MEDIUM	HIGH	In the startread function in xa.c in Sound eXchange (SoX) through 14.4.2, a corrupt header specifying zero channels triggers an infinite loop with a resultant NULL pointer dereference, which may allow a remote attacker to cause a denial-of-service.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3374
3539	CVE-2017-18187	HIGH	CRITICAL	In ARM mbed TLS before 2.7.0, there is a bounds-check bypass through an integer overflow in PSK identity parsing in the ssl_parse_client_psk_identity() function in library/ssl_srv.c.	mbedtls	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3373
3540	CVE-2017-18174	HIGH	CRITICAL	In the Linux kernel before 4.7, the amd_gpio_remove function in drivers/pinctrl/pinctrl-amd.c calls the pinctrl_unregister function, leading to a double free.	linux	Unchanged	8.0.0.26	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3435
3541	CVE-2017-18079	HIGH	High	drivers/input/serio/i8042.c in the Linux kernel before 4.12.4 allows attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact because the port->exists value can change after it is validated.	linux	Unchanged	8.0.0.26	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3222
3542	CVE-2017-18078	MEDIUM	High	systemd-tmpfiles in systemd before 237 attempts to support ownership/permission changes on hardlinked files even if the fs.protected_hardlinks sysctl is turned off, which allows local users to bypass intended access restrictions via vectors involving a hard link to a file for which the user lacks write access, as demonstrated by changing the ownership of the /etc/passwd file.	systemd	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3206
3543	CVE-2017-18075	HIGH	High	crypto/pcrypt.c in the Linux kernel before 4.14.13 mishandles freeing instances, allowing a local user able to access the AF_ALG-based AEAD interface (CONFIG_CRYPTO_USER_API_AEAD) and pcrypt (CONFIG_CRYPTO_PCRYPT) to cause a denial of service (kfree of an incorrect pointer) or possibly have unspecified other impact by executing a crafted sequence of system calls.	linux	Unchanged	Not vulnerable	9.0.0.15	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3212
3544	CVE-2017-18043	Low	Medium	Integer overflow in the macro ROUND_UP (n, d) in Quick Emulator (Qemu) allows a user to cause a denial of service (Qemu process crash).	qemu	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3349
3545	CVE-2017-18030	LOW	Medium	The cirrus_invalidate_region function in hw/display/cirrus_vga.c in Qemu allows local OS guest privileged users to cause a denial of service (out-of-bounds array access and QEMU process crash) via vectors related to negative pitch.	qemu	Unchanged	8.0.0.25	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3220
3546	CVE-2017-18029	MEDIUM	Medium	In ImageMagick 7.0.6-10 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allow remote attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3067
3547	CVE-2017-18028	HIGH	Medium	In ImageMagick 7.0.7-1 Q16, a memory exhaustion vulnerability was found in the function ReadTIFFImage in coders/tiff.c, which allow remote attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3059
3548	CVE-2017-18027	MEDIUM	Medium	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allow remote attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3062
3549	CVE-2017-18022	MEDIUM	Medium	In ImageMagick 7.0.7-12 Q16, there are memory leaks in MontageImageCommand in MagickWand/montage.c.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3106
3550	CVE-2017-18018	LOW	Medium	In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replacement of a plain file with a symlink during use of the POSIX -R -L options, which allows local users to modify the ownership of arbitrary files by leveraging a race condition.	coreutils	Unchanged	8.0.0.30	Vulnerable	10.17.41.15	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3065
3551	CVE-2017-18017	HIGH	Critical	The tcpmss_mangle_packet function in net/netfilter/xt_TCPMSS.c in the Linux kernel before 4.11, and 4.9.x before 4.9.36, allows remote attackers to cause a denial of service (use-after-free and memory corruption) or possibly have unspecified other impact by leveraging the presence of xt_TCPMSS in an iptables action.	linux	Unchanged	8.0.0.25	9.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3077
3552	CVE-2017-18013	MEDIUM	Medium	In LibTIFF 4.0.9, there is a Null-Pointer Dereference in the tif_print.c TIFFPrintDirectory function, as demonstrated by a tiffinfo crash.	libtiff	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3056
3553	CVE-2017-18009	MEDIUM	High	In OpenCV 3.3.1, a heap-based buffer over-read exists in the function cv::HdrDecoder::checkSignature in modules/imgcodecs/src/grfmt_hdr.cpp.	opencv	Unchanged	Won't Fix	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3071
3554	CVE-2017-18008	MEDIUM	Medium	In ImageMagick 7.0.7-17 Q16, there is a Memory Leak in ReadPWPImage in coders/pwp.c.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3060
3555	CVE-2017-17997	MEDIUM	High	In Wireshark 2.2.11 and before, the MRDISC dissector misuses a NULL pointer. This was addressed in epan/dissectors/packet-mrdisc.c by validating an IPv4 address. This vulnerability is similar to CVE-2017-9343.	wireshark	Unchanged	8.0.0.28	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3080
3556	CVE-2017-17975	MEDIUM	Medium	Use-after-free in the usbtv_probe function in drivers/media/usb/usbtv/usbtv-core.c in the Linux kernel through 4.14.10 allows attackers to cause a denial of service (system crash) or possibly have unspecified other impact by triggering failure of audio registration, because a kfree of the usbtv data structure occurs during a usbtv_video_free call, but the usbtv_video_fail label's code attempts to both access and free this data structure.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3055
3557	CVE-2017-17973	MEDIUM	High	In LibTIFF 4.0.8, there is a heap-based use-after-free in the t2p_writeproc function in tiff2pdf.c.	libtiff	Unchanged	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Vulnerable	LIN10-3089
3558	CVE-2017-17942	MEDIUM	High	In LibTIFF 4.0.9, there is a heap-based buffer over-read in the function PackBitsEncode in tif_packbits.c.	libtiff	Unchanged	Investigate	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN10-2942

	A	B	C	D	E	F	G	H	I	J	K	L	M
3559	CVE-2017-17935	MEDIUM	High	The File_read_line function in epan/wslua/wslua_file.c in Wireshark through 2.2.11 does not properly strip '\n' characters, which allows remote attackers to cause a denial of service (buffer underflow and application crash) via a crafted packet that triggers the attempted processing of an empty line.	wireshark	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	Won't Fix	Won't Fix	Won't Fix	LIN10-2925
3560	CVE-2017-17934	MEDIUM	Medium	ImageMagick 7.0.7-17 Q16 x86_64 has memory leaks in coders/msl.c, related to MSLPopImage and ProcessMSLScript, and associated with mishandling of MSLPushImage calls.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2961
3561	CVE-2017-17914	HIGH	Medium	In ImageMagick 7.0.7-16 Q16, a vulnerability was found in the function ReadOnePNGImage in coders/png.c, which allows attackers to cause a denial of service (ReadOneMNGImage large loop) via a crafted mng image file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2939
3562	CVE-2017-17887	MEDIUM	Medium	In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function GetImagePixelCache in magick/cache.c, which allows attackers to cause a denial of service via a crafted MNG image file that is processed by ReadOneMNGImage.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2932
3563	CVE-2017-17886	MEDIUM	Medium	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPSDChannelZip in coders/psd.c, which allows attackers to cause a denial of service via a crafted psd image file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2940
3564	CVE-2017-17884	MEDIUM	Medium	In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function WriteOnePNGImage in coders/png.c, which allows attackers to cause a denial of service via a crafted PNG image file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2938
3565	CVE-2017-17883	MEDIUM	Medium	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPGXImage in coders/pgx.c, which allows attackers to cause a denial of service via a crafted PGX image file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2949
3566	CVE-2017-17882	MEDIUM	Medium	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadXPMImage in coders/xpm.c, which allows attackers to cause a denial of service via a crafted XPM image file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2948
3567	CVE-2017-17881	MEDIUM	Medium	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted MAT image file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2941
3568	CVE-2017-17880	MEDIUM	High	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-21, there is a stack-based buffer over-read in WriteWEBPImage in coders/webp.c, related to a WEBP_DECODER_ABI_VERSION check.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-2922
3569	CVE-2017-17879	MEDIUM	High	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-21, there is a heap-based buffer over-read in ReadOneMNGImage in coders/png.c, related to length calculation and caused by an off-by-one error.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2919
3570	CVE-2017-17864	LOW	Low	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 mishandles states_equal comparisons between the pointer data type and the UNKNOWN_VALUE data type, which allows local users to obtain potentially sensitive address information, aka a pointer leak.	linux	Unchanged	8.0.0.27	9.0.0.16	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2967
3571	CVE-2017-17863	HIGH	High	kernel/bpf/verifier.c in the Linux kernel 4.9.x through 4.9.71 does not check the relationship between pointer values and the BPF stack, which allows local users to cause a denial of service (integer overflow or invalid memory access) or possibly have unspecified other impact.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2951
3572	CVE-2017-17862	MEDIUM	Medium	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 ignores unreachable code, even though it would still be processed by JIT compilers. This behavior, also considered an improper branch-pruning logic issue, could possibly be used by local users for denial of service.	linux	Unchanged	8.0.0.26	9.0.0.18	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2956
3573	CVE-2017-17857	HIGH	High	The check_stack_boundary function in kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging mishandling of invalid variable stack read operations.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2934
3574	CVE-2017-17856	HIGH	High	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging the lack of stack-pointer alignment enforcement.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2913
3575	CVE-2017-17855	HIGH	High	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging improper use of pointers in place of scalars.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2953
3576	CVE-2017-17854	HIGH	High	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (integer overflow and memory corruption) or possibly have unspecified other impact by leveraging unrestricted integer values for pointer arithmetic.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2926
3577	CVE-2017-17853	HIGH	High	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging incorrect BPF_RSH signed bounds calculations.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2966
3578	CVE-2017-17852	HIGH	High	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging mishandling of 32-bit ALU ops.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2964

	A	B	C	D	E	F	G	H	I	J	K	L	M
3579	CVE-2017-17840	MEDIUM	High	An issue was discovered in Open-iSCSI through 2.0.875. A local attacker can cause the iscsiuio server to abort or potentially execute code by sending messages with incorrect lengths, which (due to lack of checking) can lead to buffer overflows, and result in aborts (with overflow checking enabled) or code execution. The process_iscsid_broadcast function in iscsiuio/src/unix/iscsid_ipc.c does not validate the payload length before a write operation.	open-iscsi	Unchanged	Investigate	Not vulnerable	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2960
3580	CVE-2017-17821	HIGH	Critical	WTF/wtf/FastBitVector.h in WebKit, as distributed in Safari Technology Preview Release 46, allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact because it calls the FastBitVectorWordOwner::resizeSlow function (in WTF/wtf/FastBitVector.cpp) for a purpose other than initializing a bitvector size, and resizeSlow mishandles cases where the old array length is greater than the new array length.	webkit	Unchanged	Investigate	Investigate	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2915
3581	CVE-2017-17820	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is a use-after-free in pp_list_one_macro in asm/preproc.c that will lead to a remote denial of service attack, related to mishandling of operand-type errors.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2946
3582	CVE-2017-17819	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is an illegal address access in the function find_cc() in asm/preproc.c that will cause a remote denial of service attack, because pointers associated with skip_white_ calls are not validated.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2927
3583	CVE-2017-17818	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is a heap-based buffer over-read that will cause a remote denial of service attack, related to a while loop in paste_tokens in asm/preproc.c.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2916
3584	CVE-2017-17817	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is a use-after-free in pp_verror in asm/preproc.c that will cause a remote denial of service attack.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2935
3585	CVE-2017-17816	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is a use-after-free in pp_getline in asm/preproc.c that will cause a remote denial of service attack.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2923
3586	CVE-2017-17815	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is an illegal address access in is_mmacro() in asm/preproc.c that will cause a remote denial of service attack, because of a missing check for the relationship between minimum and maximum parameter counts.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2963
3587	CVE-2017-17814	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is a use-after-free in do_directive in asm/preproc.c that will cause a remote denial of service attack.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2918
3588	CVE-2017-17813	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is a use-after-free in the pp_list_one_macro function in asm/preproc.c that will cause a remote denial of service attack, related to mishandling of line-syntax errors.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2937
3589	CVE-2017-17812	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is a heap-based buffer over-read in the function detoken() in asm/preproc.c that will cause a remote denial of service attack.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2955
3590	CVE-2017-17811	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is a heap-based buffer overflow that will cause a remote denial of service attack, related to a strcpy in paste_tokens in asm/preproc.c, a similar issue to CVE-2017-11111.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2928
3591	CVE-2017-17810	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is a SEGV on unknown address that will cause a remote denial of service attack, because asm/preproc.c mishandles macro calls that have the wrong number of arguments.	nasm	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2910
3592	CVE-2017-17807	LOW	Low	The KEYS subsystem in the Linux kernel before 4.14.6 omitted an access-control check when adding a key to the current task's default request-key keyring via the request_key() system call, allowing a local user to use a sequence of crafted system calls to add keys to a keyring with only Search permission (not Write permission) to that keyring, related to construct_get_dest_keyring() in security/keys/request_key.c.	linux	Unchanged	8.0.0.26	9.0.0.15	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2929
3593	CVE-2017-17806	HIGH	High	The HMAC implementation (crypto/hmac.c) in the Linux kernel before 4.14.8 does not validate that the underlying cryptographic hash algorithm is unkeyed, allowing a local attacker able to use the AF_ALG-based hash interface (CONFIG_CRYPTO_USER_API_HASH) and the SHA-3 hash algorithm (CONFIG_CRYPTO_SHA3) to cause a kernel stack buffer overflow by executing a crafted sequence of system calls that encounter a missing SHA-3 initialization.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2936
3594	CVE-2017-17805	HIGH	High	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a denial of service (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequence of system calls that use the blkcipher_walk API. Both the generic implementation (crypto/salsa20_generic.c) and x86 implementation (arch/x86/crypto/salsa20_glue.c) of Salsa20 were vulnerable.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2950
3595	CVE-2017-17790	HIGH	Critical	The lazy_initialize function in lib/resolv.rb in Ruby through 2.4.3 uses Kernel#open, which might allow Command Injection attacks, as demonstrated by a Resolv::Hosts::new argument beginning with a '|' character, a different vulnerability than CVE-2017-17405. NOTE: situations with untrusted input may be highly unlikely.	ruby	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2947
3596	CVE-2017-17789	MEDIUM	High	In GIMP 2.8.22, there is a heap-based buffer overflow in read_channel_data in plug-ins/common/file-psp.c.	gimp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2959
3597	CVE-2017-17788	MEDIUM	High	In GIMP 2.8.22, there is a stack-based buffer over-read in xcf_load_stream in app/xcf/xcf.c when there is no '\0' character after the version string.	gimp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2914

	A	B	C	D	E	F	G	H	I	J	K	L	M
3598	CVE-2017-17787	MEDIUM	High	In GIMP 2.8.22, there is a heap-based buffer over-read in read_creator_block in plug-ins/common/file-psp.c.	gimp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2954
3599	CVE-2017-17786	MEDIUM	High	In GIMP 2.8.22, there is a heap-based buffer over-read in ReadImage in plug-ins/common/file-tga.c (related to bgr2rgb.part.1) via an unexpected bits-per-pixel value for an RGBA image.	gimp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2957
3600	CVE-2017-17785	MEDIUM	High	In GIMP 2.8.22, there is a heap-based buffer overflow in the fli_read_brun function in plug-ins/file-fli/fli.c.	gimp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2943
3601	CVE-2017-17784	MEDIUM	High	In GIMP 2.8.22, there is a heap-based buffer over-read in load_image in plug-ins/common/file-gbr.c in the gbr import parser, related to mishandling of UTF-8 data.	gimp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2958
3602	CVE-2017-17760	MEDIUM	High	OpenCV 3.3.1 has a Buffer Overflow in the cv::PxMDecoder::readData function in grfmt_pxm.cpp, because an incorrect size value is used.	opencv	Unchanged	Won't Fix	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3069
3603	CVE-2017-17742	MEDIUM	MEDIUM	Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1 allows an HTTP Response Splitting attack. An attacker can inject a crafted key and value into an HTTP response for the HTTP server of WEBrick.	ruby	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3738
3604	CVE-2017-17741	LOW	Medium	The KVM implementation in the Linux kernel through 4.14.7 allows attackers to cause a denial of service (write_mmio stack-based out-of-bounds read) or possibly have unspecified other impact, related to arch/x86/kvm/x86.c and include/trace/events/kvm.h.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2921
3605	CVE-2017-17740	MEDIUM	High	contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module and the memberof overlay are enabled, attempts to free a buffer that was allocated on the stack, which allows remote attackers to cause a denial of service (slapd crash) via a member MODDN operation.	openldap	Unchanged	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	Investigate	LIN10-2817
3606	CVE-2017-17712	MEDIUM	High	The raw_sendmsg() function in net/ipv4/raw.c in the Linux kernel through 4.14.6 has a race condition in inet->hdrincl that leads to uninitialized stack pointer usage; this allows a local user to execute code and gain privileges.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2796
3607	CVE-2017-17682	HIGH	Medium	In ImageMagick 7.0.7-12 Q16, a large loop vulnerability was found in the function ExtractPostscript in coders/wpg.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted wpg image file that triggers a ReadWPGImage call.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2758
3608	CVE-2017-17681	HIGH	Medium	In ImageMagick 7.0.7-12 Q16, an infinite loop vulnerability was found in the function ReadPSDChannelZip in coders/psd.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted psd image file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2750
3609	CVE-2017-17680	MEDIUM	Medium	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadXPMImage in coders/xpm.c, which allows attackers to cause a denial of service via a crafted xpm image file.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2770
3610	CVE-2017-17558	HIGH	Medium	The usb_destroy_configuration function in drivers/usb/core/config.c in the USB core subsystem in the Linux kernel through 4.14.5 does not consider the maximum number of configurations and interfaces before attempting to release resources, which allows local users to cause a denial of service (out-of-bounds write access) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2782
3611	CVE-2017-17555	MEDIUM	Medium	The swri_audio_convert function in audioconvert.c in FFmpeg libswresample through 3.0.101, as used in FFmpeg 3.4.1, aubio 0.4.6, and other products, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted audio file.	ffmpeg	Unchanged	Not vulnerable	Vulnerable	Investigate	Investigate	Not vulnerable	Not vulnerable	LIN10-2749
3612	CVE-2017-17529	MEDIUM	High	af/util/xp/ut_go_file.cpp in AbiWord 3.0.2-2 does not validate strings before launching the program specified by the BROWSER environment variable, which might allow remote attackers to conduct argument-injection attacks via a crafted URL.	abiword	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2965
3613	CVE-2017-17522	MEDIUM	High	Lib/webbrowser.py in Python through 3.6.3 does not validate strings before launching the program specified by the BROWSER environment variable, which might allow remote attackers to conduct argument-injection attacks via a crafted URL.	python	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2952
3614	CVE-2017-17521	MEDIUM	High	uiutil.c in FontForge through 20170731 does not validate strings before launching the program specified by the BROWSER environment variable, which might allow remote attackers to conduct argument-injection attacks via a crafted URL, a different vulnerability than CVE-2017-17534.	fontforge	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2962
3615	CVE-2017-17504	MEDIUM	Medium	ImageMagick before 7.0.7-12 has a coders/png.c Magick_png_read_raw_profile heap-based buffer over-read via a crafted file, related to ReadOneMNGImage.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2745
3616	CVE-2017-17499	HIGH	Critical	ImageMagick before 6.9.9-24 and 7.x before 7.0.7-12 has a use-after-free in Magick::Image::read in Magick++/lib/Image.cpp.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2771
3617	CVE-2017-17484	HIGH	Critical	The ucnv_UTF8FromUTF8 function in ucnv_u8.cpp in International Components for Unicode (ICU) for C/C++ through 60.1 mishandles ucnv_convertEx calls for UTF-8 to UTF-8 conversion, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted string, as demonstrated by ZNC.	icu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2755
3618	CVE-2017-17480	HIGH	Critical	In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the pgxtovolume function in jp3d/convert.c. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly remote code execution.	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2759
3619	CVE-2017-17479	HIGH	Critical	In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the pgxtoimage function in jpwl/convert.c. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly remote code execution.	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2778

	A	B	C	D	E	F	G	H	I	J	K	L	M
3620	CVE-2017-17458	HIGH	Critical	In Mercurial before 4.4.1, it is possible that a specially malformed repository can cause Git subrepositories to run arbitrary code in the form of a .git/hooks/post-update script checked into the repository. Typical use of Mercurial prevents construction of such repositories, but they can be created programmatically.	mercurial	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2762
3621	CVE-2017-17457	MEDIUM	Medium	The function d2ulaw_array() in ulaw.c of libsndfile 1.0.29pre1 may lead to a remote DoS attack (SEGV on unknown address 0x000000000000), a different vulnerability than CVE-2017-14246.	libsndfile	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	10.19.45.1	Not vulnerable	LIN10-2763
3622	CVE-2017-17456	MEDIUM	Medium	The function d2alaw_array() in alaw.c of libsndfile 1.0.29pre1 may lead to a remote DoS attack (SEGV on unknown address 0x000000000000), a different vulnerability than CVE-2017-14245.	libsndfile	Unchanged	8.0.0.30	9.0.0.20	10.17.41.15	10.18.44.4	10.19.45.1	Not vulnerable	LIN10-2776
3623	CVE-2017-17450	MEDIUM	High	net/netfilter/xt_osf.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for add_callback and remove_callback operations, which allows local users to bypass intended access restrictions because the xt_osf_fingers data structure is shared across all net namespaces.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2757
3624	CVE-2017-17449	LOW	Medium	The __netlink_deliver_tap_skb function in net/netlink/af_netlink.c in the Linux kernel through 4.14.4, when CONFIG_NLMON is enabled, does not restrict observations of Netlink messages to a single net namespace, which allows local users to obtain sensitive information by leveraging the CAP_NET_ADMIN capability to sniff an nlmon interface for all Netlink activity on the system.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2760
3625	CVE-2017-17448	MEDIUM	High	net/netfilter/nfnetlink_cthelper.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for new, get, and del operations, which allows local users to bypass intended access restrictions because the nfnl_cthelper_list data structure is shared across all net namespaces.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2756
3626	CVE-2017-17434	HIGH	Critical	The daemon in rsync 3.1.2, and 3.1.3-development before 2017-12-03, does not check for fnamecmp filenames in the daemon_filter_list data structure (in the recv_files function in receiver.c) and also does not apply the sanitize_paths protection mechanism to pathnames found in xname follows strings (in the read_ndx_and_attrs function in rsync.c), which allows remote attackers to bypass intended access restrictions.	rsync	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2737
3627	CVE-2017-17433	HIGH	Critical	The recv_files function in receiver.c in the daemon in rsync 3.1.2, and 3.1.3-development before 2017-12-03, proceeds with certain file metadata updates before checking for a filename in the daemon_filter_list data structure, which allows remote attackers to bypass intended access restrictions.	rsync	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2736
3628	CVE-2017-17426	MEDIUM	High	The malloc function in the GNU C Library (aka glibc or libc6) 2.26 could return a memory block that is too small if an attempt is made to allocate an object whose size is close to SIZE_MAX, potentially leading to a subsequent heap overflow. This occurs because the per-thread cache (aka tcache) feature enables a code path that lacks an integer overflow check.	glibc	Unchanged	Not vulnerable	Not vulnerable	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2780
3629	CVE-2017-17405	HIGH	High	Ruby before 2.4.3 allows Net::FTP command injection. Net::FTP#get, getbinaryfile, gettextfile, put, putbinaryfile, and puttextfile use Kernel#open to open a local file. If the localfile argument starts with the | pipe character, the command following the pipe character is executed. The default value of localfile is File.basename(remotefile), so malicious FTP servers could cause arbitrary command execution.	ruby	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2930
3630	CVE-2017-17381	LOW	Medium	The Virtio Vring implementation in QEMU allows local OS guest users to cause a denial of service (divide-by-zero error and QEMU process crash) by unsetting vring alignment while updating Virtio rings.	qemu	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2738
3631	CVE-2017-17130	MEDIUM	High	The ff_free_picture_tables function in libavcodec/mpegpicture.c in Libav 12.2 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file, related to vc1_decode_i_blocks_adv.	libav	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-2746
3632	CVE-2017-17129	MEDIUM	High	The ff_vc1_mc_4mv_chroma4 function in libavcodec/vc1_mc.c in Libav 12.2 allows remote attackers to cause a denial of service (segmentation fault and application crash) or possibly have unspecified other impact via a crafted file.	libav	Unchanged	Vulnerable	9.0.0.19	10.17.41.13	Won't Fix	Won't Fix	Won't Fix	LIN10-2777
3633	CVE-2017-17128	MEDIUM	Medium	The h264_slice_init function in libavcodec/h264_slice.c in Libav 12.2 allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted file.	libav	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-2781
3634	CVE-2017-17127	MEDIUM	Medium	The vc1_decode_frame function in libavcodec/vc1dec.c in Libav 12.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file.	libav	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-2754
3635	CVE-2017-17126	MEDIUM	High	The load_debug_section function in readelf.c in GNU Binutils 2.29.1 allows remote attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified other impact via an ELF file that lacks section headers.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2764
3636	CVE-2017-17125	MEDIUM	High	nm.c and objdump.c in GNU Binutils 2.29.1 mishandle certain global symbols, which allows remote attackers to cause a denial of service (_bfd_elf_get_symbol_version_string buffer over-read and application crash) or possibly have unspecified other impact via a crafted ELF file.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2742
3637	CVE-2017-17124	MEDIUM	High	The _bfd_coff_read_string_table function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not properly validate the size of the external string table, which allows remote attackers to cause a denial of service (excessive memory consumption, or heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted COFF binary.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2772

	A	B	C	D	E	F	G	H	I	J	K	L	M
3638	CVE-2017-17123	MEDIUM	Medium	The coff_slurp_reloc_table function in coffcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted COFF based file.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2753
3639	CVE-2017-17122	MEDIUM	High	The dump_relocs_in_section function in objdump.c in GNU Binutils 2.29.1 does not check for reloc count integer overflows, which allows remote attackers to cause a denial of service (excessive memory allocation, or heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PE file.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2774
3640	CVE-2017-17121	MEDIUM	High	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (memory access violation) or possibly have unspecified other impact via a COFF binary in which a relocation refers to a location after the end of the to-be-relocated section.	binutils	Unchanged	8.0.0.25	9.0.0.15	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2769
3641	CVE-2017-17095	MEDIUM	High	tools/pal2rgb.c in pal2rgb in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (TIFFSetupStrips heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted TIFF file.	libtiff	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2740
3642	CVE-2017-17089	LOW	Medium	custom/run.cgi in Webmin before 1.870 allows remote authenticated administrators to conduct XSS attacks via the description field in the custom command functionality.	webmin	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3092
3643	CVE-2017-17087	LOW	Medium	fileio.c in Vim prior to 8.0.1263 sets the group ownership of a .swp file to the editor's primary group (which may be different from the group ownership of the original file), which allows local users to obtain sensitive information by leveraging an applicable group membership, as demonstrated by /etc/shadow owned by root:shadow mode 0640, but /etc/.shadow.swp owned by root:users mode 0640, a different vulnerability than CVE-2017-1000382.	vim	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2751
3644	CVE-2017-17085	MEDIUM	High	In Wireshark 2.4.0 to 2.4.2 and 2.2.0 to 2.2.10, the CIP Safety dissector could crash. This was addressed in epan/dissectors/packet-cipsafety.c by validating the packet length.	wireshark	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2741
3645	CVE-2017-17084	MEDIUM	High	In Wireshark 2.4.0 to 2.4.2 and 2.2.0 to 2.2.10, the IWARP_MPA dissector could crash. This was addressed in epan/dissectors/packet-iwarp-mpa.c by validating a ULPDU length.	wireshark	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2773
3646	CVE-2017-17083	MEDIUM	High	In Wireshark 2.4.0 to 2.4.2 and 2.2.0 to 2.2.10, the NetBIOS dissector could crash. This was addressed in epan/dissectors/packet-netbios.c by ensuring that write operations are bounded by the beginning of a buffer.	wireshark	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2752
3647	CVE-2017-17081	MEDIUM	Medium	The gmc_mmx function in libavcodec/x86/mpegvideodsp.c in FFmpeg 3.4 does not properly validate widths and heights, which allows remote attackers to cause a denial of service (integer signedness error and out-of-array read) via a crafted MPEG file.	ffmpeg	Unchanged	Not vulnerable	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2766
3648	CVE-2017-17080	MEDIUM	Medium	elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate sizes of core notes, which allows remote attackers to cause a denial of service (bfd_getl32 heap-based buffer over-read and application crash) via a crafted object file, related to elfcore_grok_netbsd_procinfo, elfcore_grok_openbsd_procinfo, and elfcore_grok_nto_status.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2775
3649	CVE-2017-17053	HIGH	High	The init_new_context function in arch/x86/include/asm/mmu_context.h in the Linux kernel before 4.12.10 does not correctly handle errors from LDT table allocation when forking a new process, allowing a local attacker to achieve a use-after-free or possibly have unspecified other impact by running a specially crafted program. This vulnerability only affected kernels built with CONFIG_MODIFY_LDT_SYSCALL=y.	linux	Unchanged	Not vulnerable	9.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2631
3650	CVE-2017-17052	HIGH	High	The mm_init function in kernel/fork.c in the Linux kernel before 4.12.10 does not clear the ->exe_file member of a new process's mm_struct, allowing a local attacker to achieve a use-after-free or possibly have unspecified other impact by running a specially crafted program.	linux	Unchanged	8.0.0.25	9.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2640
3651	CVE-2017-17042	MEDIUM	High	lib/yard/core_ext/file.rb in the server in YARD before 0.9.11 does not block relative paths with an initial ../ sequence, which allows attackers to conduct directory traversal attacks and read arbitrary files.	yard	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2617
3652	CVE-2017-16997	HIGH	High	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH containing $ORIGIN for a privileged (setuid or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse library in the current working directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion of an empty RPATH/RUNPATH token as the ./ directory. NOTE: this configuration of RPATH/RUNPATH for a privileged program is apparently very uncommon; most likely, no such program is shipped with any common Linux distribution.	glibc	Unchanged	8.0.0.25	9.0.0.15	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2816
3653	CVE-2017-16996	HIGH	High	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging register truncation mishandling.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2917
3654	CVE-2017-16995	HIGH	High	The check_alu_op function in kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging incorrect sign extension.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2912

	A	B	C	D	E	F	G	H	I	J	K	L	M
3655	CVE-2017-16994	LOW	Medium	The walk_hugetlb_range function in mm/pagewalk.c in the Linux kernel before 4.14.2 mishandles holes in hugetlb ranges, which allows local users to obtain sensitive information from uninitialized kernel memory via crafted use of the mincore() system call.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2597
3656	CVE-2017-16942	MEDIUM	Medium	In libsndfile 1.0.25 (fixed in 1.0.26), a divide-by-zero error exists in the function wav_w64_read_fmt_chunk() in wav_w64.c, which may lead to DoS when playing a crafted audio file.	libsndfile	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2610
3657	CVE-2017-16939	HIGH	High	The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted SO_RCVBUF setsockopt system call in conjunction with XFRM_MSG_GETPOLICY Netlink messages.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2641
3658	CVE-2017-16932	MEDIUM	High	parser.c in libxml2 before 2.9.5 does not prevent infinite recursion in parameter entities.	libxml2	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2629
3659	CVE-2017-16931	HIGH	Critical	parser.c in libxml2 before 2.9.5 mishandles parameter-entity references because the NEXTL macro calls the xmlParserHandlePEReference function in the case of a '%' character in a DTD name.	libxml2	Unchanged	8.0.0.24	9.0.0.13	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2633
3660	CVE-2017-16914	High	Medium	The stub_send_ret_submit() function (drivers/usb/usbip/stub_tx.c) in the Linux Kernel before version 4.14.8, 4.9.71, 4.1.49, and 4.4.107 allows attackers to cause a denial of service (NULL pointer dereference) via a specially crafted USB over IP packet.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3414
3661	CVE-2017-16913	High	Medium	The stub_recv_cmd_submit() function (drivers/usb/usbip/stub_rx.c) in the Linux Kernel before version 4.14.8, 4.9.71, and 4.4.114 when handling CMD_SUBMIT packets allows attackers to cause a denial of service (arbitrary memory allocation) via a specially crafted USB over IP packet.	linux	Unchanged	8.0.0.26	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3333
3662	CVE-2017-16912	High	Medium	The get_pipe() function (drivers/usb/usbip/stub_rx.c) in the Linux Kernel before version 4.14.8, 4.9.71, and 4.4.114 allows attackers to cause a denial of service (out-of-bounds read) via a specially crafted USB over IP packet.	linux	Unchanged	8.0.0.26	9.0.0.18	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3311
3663	CVE-2017-16911	Low	Medium	The vhci_hcd driver in the Linux Kernel before version 4.14.8 and 4.4.114 allows allows local attackers to disclose kernel memory addresses. Successful exploitation requires that a USB device is attached over IP.	linux	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3359
3664	CVE-2017-16879	MEDIUM	High	Stack-based buffer overflow in the _nc_write_entry function in tinfo/write_entry.c in ncurses 6.0 allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted terminfo file, as demonstrated by tic.	ncurses	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2639
3665	CVE-2017-16845	HIGH	Critical	hw/input/ps2.c in Qemu does not validate 'rptr' and 'count' values during guest migration, leading to out-of-bounds access.	qemu	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2638
3666	CVE-2017-16840	HIGH	Critical	The VC-2 Video Compression encoder in FFmpeg 3.4 allows remote attackers to cause a denial of service (out-of-bounds read) because of incorrect buffer padding for non-Haar wavelets, related to libavcodec/vc2enc.c and libavcodec/vc2enc_dwt.c.	ffmpeg	Unchanged	Won't Fix	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2626
3667	CVE-2017-16832	MEDIUM	High	The pe_bfd_read_buildid function in peicode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate size and offset values in the data dictionary, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via a crafted PE file.	binutils	Unchanged	Not vulnerable	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2628
3668	CVE-2017-16831	MEDIUM	High	coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not validate the symbol count, which allows remote attackers to cause a denial of service (integer overflow and application crash, or excessive memory allocation) or possibly have unspecified other impact via a crafted PE file.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2622
3669	CVE-2017-16830	MEDIUM	High	The print_gnu_property_note function in readelf.c in GNU Binutils 2.29.1 does not have integer-overflow protection on 32-bit platforms, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via a crafted ELF file.	binutils	Unchanged	Not vulnerable	Not vulnerable	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2637
3670	CVE-2017-16829	MEDIUM	High	The _bfd_elf_parse_gnu_properties function in elf-properties.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, does not prevent negative pointers, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) or possibly have unspecified other impact via a crafted ELF file.	binutils	Unchanged	Not vulnerable	Not vulnerable	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2618
3671	CVE-2017-16828	MEDIUM	High	The display_debug_frames function in dwarf.c in GNU Binutils 2.29.1 allows remote attackers to cause a denial of service (integer overflow and heap-based buffer over-read, and application crash) or possibly have unspecified other impact via a crafted ELF file, related to print_debug_frame.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2630
3672	CVE-2017-16827	MEDIUM	High	The aout_get_external_symbols function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (slurp_symtab invalid free and application crash) or possibly have unspecified other impact via a crafted ELF file.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2635
3673	CVE-2017-16826	MEDIUM	High	The coff_slurp_line_table function in coffcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29.1, allows remote attackers to cause a denial of service (invalid memory access and application crash) or possibly have unspecified other impact via a crafted PE file.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2611
3674	CVE-2017-16820	HIGH	Critical	The csnmp_read_table function in snmp.c in the SNMP plugin in collectd before 5.6.3 is susceptible to a double free in a certain error case, which could lead to a crash (or potentially have other impact).	collectd	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2642

	A	B	C	D	E	F	G	H	I	J	K	L	M
3675	CVE-2017-16808	MEDIUM	Medium	tcpdump 4.9.2 has a heap-based buffer over-read related to aoe_print in print-aoe.c and lookup_emem in addrtoname.c.	tcpdump	Unchanged	8.0.0.33	9.0.0.25	10.17.41.20	10.18.44.15	10.19.45.1	Not vulnerable	LIN10-2623
3676	CVE-2017-16803	MEDIUM	High	In Libav through 11.11 and 12.x through 12.1, the smacker_decode_tree function in libavcodec/smacker.c does not properly restrict tree recursion, which allows remote attackers to cause a denial of service (bitstream.c:build_table() out-of-bounds read and application crash) via a crafted Smacker stream.	libav	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Won't Fix	Won't Fix	LIN10-2632
3677	CVE-2017-16650	HIGH	Medium	The qmi_wwan_bind function in drivers/net/usb/qmi_wwan.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (divide-by-zero error and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2481
3678	CVE-2017-16649	HIGH	Medium	The usbnet_generic_cdc_bind function in drivers/net/usb/cdc_ether.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (divide-by-zero error and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2502
3679	CVE-2017-16648	HIGH	Medium	The dvb_frontend_free function in drivers/media/dvb-core/dvb_frontend.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via a crafted USB device. NOTE: the function was later renamed __dvb_frontend_free.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2479
3680	CVE-2017-16647	HIGH	Medium	drivers/net/usb/asix_devices.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	Won't Fix	Won't Fix	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2482
3681	CVE-2017-16646	HIGH	Medium	drivers/media/usb/dvb-usb/dib0700_devices.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (BUG and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2508
3682	CVE-2017-16645	HIGH	Medium	The ims_pcu_get_cdc_union_desc function in drivers/input/misc/ims-pcu.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (ims_pcu_parse_cdc_data out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2495
3683	CVE-2017-16644	HIGH	Medium	The hdpvr_probe function in drivers/media/usb/hdpvr/hdpvr-core.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (improper error handling and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2483
3684	CVE-2017-16643	HIGH	Medium	The parse_hid_report_descriptor function in drivers/input/tablet/gtco.c in the Linux kernel before 4.13.11 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2497
3685	CVE-2017-16642	MEDIUM	High	In PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11, an error in the date extension's timelib_meridian handling of 'front of' and 'back of' directives could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this is a different issue than CVE-2017-11145.	php	Unchanged	8.0.0.24	9.0.0.13	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2506
3686	CVE-2017-16612	MEDIUM	High	libXcursor before 1.1.15 has various integer overflows that could lead to heap buffer overflows when processing malicious cursors, e.g., with programs like GIMP.	libxcursor	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2779
3687	CVE-2017-16611	LOW	Medium	In libXfont before 1.5.4 and libXfont2 before 2.0.3, a local attacker can open (but not read) files on the system as root, triggering tape rewinds, watchdogs, or similar mechanisms that can be triggered by opening files.	libxfont	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2743
3688	CVE-2017-16548	HIGH	Critical	The receive_xattr function in xattrs.c in rsync 3.1.2 and 3.1.3-development does not check for a trailing \0 character in an xattr name, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact by sending crafted data to the daemon.	rsync	Unchanged	8.0.0.24	9.0.0.13	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2490
3689	CVE-2017-16546	MEDIUM	High	The ReadWPGImage function in coders/wpg.c in ImageMagick 7.0.7-9 does not properly validate the colormap index in a WPG palette, which allows remote attackers to cause a denial of service (use of uninitialized data or invalid memory allocation) or possibly have unspecified other impact via a malformed WPG file.	imagemagick	Unchanged	8.0.0.24	9.0.0.13	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2484
3690	CVE-2017-16544	MEDIUM	High	In the add_match function in libbb/lineedit.c in BusyBox through 1.27.2, the tab autocomplete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal. This could potentially result in code execution, arbitrary file writes, or other attacks.	busybox	Unchanged	8.0.0.24	9.0.0.13	10.17.41.2	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2620
3691	CVE-2017-16538	HIGH	Medium	drivers/media/usb/dvb-usb-v2/lmedm04.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (general protection fault and system crash) or possibly have unspecified other impact via a crafted USB device, related to a missing warm-start check and incorrect attach timing (dm04_lme2510_frontend_attach versus dm04_lme2510_tuner).	linux	Unchanged	8.0.0.26	9.0.0.15	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2512
3692	CVE-2017-16537	HIGH	Medium	The imon_probe function in drivers/media/rc/imon.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.25	9.0.0.15	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2494

	A	B	C	D	E	F	G	H	I	J	K	L	M
3693	CVE-2017-16536	HIGH	Medium	The cx231xx_usb_probe function in drivers/media/usb/cx231xx/cx231xx-cards.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.25	9.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2500
3694	CVE-2017-16535	HIGH	Medium	The usb_get_bos_descriptor function in drivers/usb/core/config.c in the Linux kernel before 4.13.10 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2511
3695	CVE-2017-16534	HIGH	Medium	The cdc_parse_cdc_header function in drivers/usb/core/message.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	Not vulnerable	9.0.0.15	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2499
3696	CVE-2017-16533	HIGH	Medium	The usbhid_parse function in drivers/hid/usbhid/hid-core.c in the Linux kernel before 4.13.8 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2503
3697	CVE-2017-16532	HIGH	Medium	The get_endpoints function in drivers/usb/misc/usbtest.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.30	9.0.0.14	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2473
3698	CVE-2017-16531	HIGH	Medium	drivers/usb/core/config.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device, related to the USB_DT_INTERFACE_ASSOCIATION descriptor.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2496
3699	CVE-2017-16530	HIGH	Medium	The uas driver in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device, related to drivers/usb/storage/uas-detect.h and drivers/usb/storage/uas.c.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2510
3700	CVE-2017-16529	HIGH	Medium	The snd_usb_create_streams function in sound/usb/card.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2486
3701	CVE-2017-16528	HIGH	Medium	sound/core/seq_device.c in the Linux kernel before 4.13.4 allows local users to cause a denial of service (snd_rawmidi_dev_seq_free use-after-free and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2476
3702	CVE-2017-16527	HIGH	Medium	sound/usb/mixer.c in the Linux kernel before 4.13.8 allows local users to cause a denial of service (snd_usb_mixer_interrupt use-after-free and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2498
3703	CVE-2017-16526	HIGH	High	drivers/uwb/uwbd.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (general protection fault and system crash) or possibly have unspecified other impact via a crafted USB device.	linux	Unchanged	8.0.0.27	9.0.0.18	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2485
3704	CVE-2017-16525	HIGH	Medium	The usb_serial_console_disconnect function in drivers/usb/serial/console.c in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via a crafted USB device, related to disconnection and failed setup.	linux	Unchanged	8.0.0.25	9.0.0.15	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2471
3705	CVE-2017-16516	MEDIUM	High	In the yajl-ruby gem 1.3.0 for Ruby, when a crafted JSON file is supplied to Yajl::Parser.new.parse, the whole ruby process crashes with a SIGABRT in the yajl_string_decode function in yajl_encode.c. This results in the whole ruby process terminating and potentially a denial of service.	yajl-ruby	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2472
3706	CVE-2017-16232	MEDIUM	HIGH	tools/tiff2bw.c (main): Free memory allocated in the tiff2bw Program.	libtiff	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3068
3707	CVE-2017-16227	MEDIUM	High	The aspath_put function in bgpd/bgp_aspath.c in Quagga before 1.2.2 allows remote attackers to cause a denial of service (session drop) via BGP UPDATE messages, because AS_PATH size calculation for long paths counts certain bytes twice and consequently constructs an invalid message.	quagga	Unchanged	8.0.0.24	9.0.0.13	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2507
3708	CVE-2017-15996	MEDIUM	High	elfcomm.c in readelf in GNU Binutils 2.29 allows remote attackers to cause a denial of service (excessive memory allocation) or possibly have unspecified other impact via a crafted ELF file that triggers a buffer overflow on fuzzed archive header, related to an uninitialized variable, an improper conditional jump, and the get_archive_member_name, process_archive_index_and_symbols, and setup_archive functions.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.8	Vulnerable	Vulnerable	Vulnerable	LIN9-5773
3709	CVE-2017-15994	HIGH	Critical	rsync 3.1.3-development before 2017-10-24, as used in the xlucas svfs rsync fork and other products, mishandles archaic checksums, which makes it easier for remote attackers to bypass intended access restrictions.	rsync	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5689
3710	CVE-2017-15951	HIGH	High	The KEYS subsystem in the Linux kernel before 4.13.10 does not correctly synchronize the actions of updating versus finding a key in the negative state to avoid a race condition, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5673
3711	CVE-2017-15939	MEDIUM	Medium	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles NULL files in a .debug_line file table, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to concat_filename. NOTE: this issue is caused by an incomplete fix for CVE-2017-15023.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5678

	A	B	C	D	E	F	G	H	I	J	K	L	M
3712	CVE-2017-15938	MEDIUM	High	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, miscalculates DW_FORM_ref_addr die refs in the case of a relocatable object file, which allows remote attackers to cause a denial of service (find_abstract_instance_name invalid memory read, segmentation fault, and application crash).	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5734
3713	CVE-2017-15908	MEDIUM	High	In systemd 223 through 235, a remote DNS server can respond with a custom crafted DNS NSEC resource record to trigger an infinite loop in the dns_packet_read_type_window() function of the 'systemd-resolved' service and cause a DoS of the affected service.	systemd	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5692
3714	CVE-2017-15906	MEDIUM	Medium	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.	openssh	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5676
3715	CVE-2017-15874	MEDIUM	Medium	archival/libarchive/decompress_unlzma.c in BusyBox 1.27.2 has an Integer Underflow that leads to a read access violation.	busybox	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5730
3716	CVE-2017-15873	MEDIUM	Medium	The get_next_block function in archival/libarchive/decompress_bunzip2.c in BusyBox 1.27.2 has an Integer Overflow that may lead to a write access violation.	busybox	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5700
3717	CVE-2017-15868	HIGH	High	The bnep_add_connection function in net/bluetooth/bnep/core.c in the Linux kernel before 3.19 does not ensure that an l2cap socket is available, which allows local users to gain privileges via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2739
3718	CVE-2017-15804	High	Critical	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.	glibc	Unchanged	8.0.0.25	9.0.0.12	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5731
3719	CVE-2017-15723	Medium	High	In Irssi before 1.0.5, overlong nicks or targets may result in a NULL pointer dereference while splitting the message.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5715
3720	CVE-2017-15722	Medium	High	In certain cases, Irssi before 1.0.5 may fail to verify that a Safe channel ID is long enough, causing reads beyond the end of the string.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5697
3721	CVE-2017-15721	Medium	High	In Irssi before 1.0.5, certain incorrectly formatted DCC CTCP messages could cause a NULL pointer dereference. This is a separate, but similar, issue relative to CVE-2017-9468.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5685
3722	CVE-2017-15715	MEDIUM	HIGH	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.	apache	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3652
3723	CVE-2017-15710	MEDIUM	HIGH	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.	apache	Unchanged	8.0.0.26	9.0.0.16	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3638
3724	CVE-2017-15672	MEDIUM	High	The read_header function in libavcodec/ffv1dec.c in FFmpeg 3.3.4 and earlier allows remote attackers to have unspecified impact via a crafted MP4 file, which triggers an out-of-bounds read.	ffmpeg	Unchanged	Won't Fix	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2477
3725	CVE-2017-15671	Medium	Medium	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27, when invoked with GLOB_TILDE, could skip freeing allocated memory when processing the ~ operator with a long user name, potentially leading to a denial of service (memory leak).	glibc	Unchanged	8.0.0.25	9.0.0.12	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5629
3726	CVE-2017-15670	High	Critical	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.	glibc	Unchanged	8.0.0.25	9.0.0.12	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5623
3727	CVE-2017-15652	Medium	MEDIUM	Artifex Ghostscript 9.22 is affected by: Obtain Information. The impact is: obtain sensitive information. The component is: affected source code file, affected function, affected executable, affected libga (imagemagick used that). The attack vector is: Someone must open a postscript file though ghostscript. Because of imagemagick also use libga, so it was affected as well.	ghostscript	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4152
3728	CVE-2017-15650	MEDIUM	High	musl libc before 1.1.17 has a buffer overflow via crafted DNS replies because dns_parse_callback in network/lookup_name.c does not restrict the number of addresses, and thus an attacker can provide an unexpected number by sending A records in a reply to an AAAA query.	musl	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5727
3729	CVE-2017-15649	MEDIUM	High	net/packet/af_packet.c in the Linux kernel before 4.13.6 allows local users to gain privileges via crafted system calls that trigger mishandling of packet_fanout data structures, because of a race condition (involving fanout_add and packet_do_bind) that leads to a use-after-free, a different vulnerability than CVE-2017-6346.	linux	Unchanged	8.0.0.23	9.0.0.13	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5723
3730	CVE-2017-15644	MEDIUM	High	SSRF exists in Webmin 1.850 via the PATH_INFO to tunnel/link.cgi, as demonstrated by a GET request for tunnel/link.cgi/http://INTRANET-IP:8000.	webmin	Unchanged	8.0.0.23	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5717
3731	CVE-2017-15642	MEDIUM	Medium	In lsx_aiffstartread in aiff.c in Sound eXchange (SoX) 14.4.2, there is a Use-After-Free vulnerability triggered by supplying a malformed AIFF file.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5713

	A	B	C	D	E	F	G	H	I	J	K	L	M
3732	CVE-2017-15565	Medium	High	In Poppler 0.59.0, a NULL Pointer Dereference exists in the GfxImageColorMap::getGrayLine() function in GfxState.cc via a crafted PDF document.	poppler	Unchanged	Won't Fix	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5690
3733	CVE-2017-15537	LOW	Medium	The x86/fpu (Floating Point Unit) subsystem in the Linux kernel before 4.13.5, when a processor supports the xsave feature but not the xsaves feature, does not correctly handle attempts to set reserved bits in the xstate header via the ptrace() or rt_sigreturn() system call, allowing local users to read the FPU registers of other processes on the system, related to arch/x86/kernel/fpu/regset.c and arch/x86/kernel/fpu/signal.c.	linux	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5712
3734	CVE-2017-15535	MEDIUM	Critical	MongoDB 3.4.x before 3.4.10, and 3.5.x-development, has a disabled-by-default configuration setting, networkMessageCompressors (aka wire protocol compression), which exposes a vulnerability when enabled that could be exploited by a malicious attacker to deny service or modify memory.	mongodb	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2478
3735	CVE-2017-15412	MEDIUM	HIGH	Use after free in libxml2 before 2.9.5, as used in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	libxml2	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4634
3736	CVE-2017-15377	MEDIUM	High	In Suricata before 4.x, it was possible to trigger lots of redundant checks on the content of crafted network traffic with a certain signature, because of DetectEngineContentInspection in detect-engine-content-inspection.c. The search engine doesn't stop when it should after no match is found; instead, it stops only upon reaching inspection-recursion-limit (3000 by default).	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5674
3737	CVE-2017-15372	MEDIUM	Medium	There is a stack-based buffer overflow in the lsx_ms_adpcm_block_expand_i function of adpcm.c in Sound eXchange (SoX) 14.4.2. A Crafted input will lead to a denial of service attack during conversion of an audio file.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5591
3738	CVE-2017-15371	MEDIUM	Medium	There is a reachable assertion abort in the function sox_append_comment() in formats.c in Sound eXchange (SoX) 14.4.2. A Crafted input will lead to a denial of service attack during conversion of an audio file.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5534
3739	CVE-2017-15370	MEDIUM	Medium	There is a heap-based buffer overflow in the ImaExpandS function of ima_rw.c in Sound eXchange (SoX) 14.4.2. A Crafted input will lead to a denial of service attack during conversion of an audio file.	sox	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5588
3740	CVE-2017-15365	MEDIUM	High	sql/event_data_objects.cc in MariaDB before 10.1.30 and 10.2.x before 10.2.10 and Percona XtraDB Cluster before 5.6.37-26.21-3 and 5.7.x before 5.7.19-29.22-3 allows remote authenticated users with SQL access to bypass intended access restrictions and replicate data definition language (DDL) statements to cluster nodes by leveraging incorrect ordering of DDL replication and ACL checking.	mariadb	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3190
3741	CVE-2017-15306	MEDIUM	Medium	The kvm_vm_ioctl_check_extension function in arch/powerpc/kvm/powerpc.c in the Linux kernel before 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) via a KVM_CHECK_EXTENSION KVM_CAP_PPC_HTM ioctl call to /dev/kvm.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2491
3742	CVE-2017-15299	MEDIUM	Medium	The KEYS subsystem in the Linux kernel through 4.13.7 mishandles use of add_key for a key that already exists but is uninstantiated, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted system call.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5575
3743	CVE-2017-15298	MEDIUM	Medium	Git through 2.14.2 mishandles layers of tree objects, which allows remote attackers to cause a denial of service (memory consumption) via a crafted repository, aka a Git bomb. This can also have an impact of disk consumption; however, an affected process typically would not survive its attempt to build the data structure in memory before writing to disk.	git	Unchanged	8.0.0.30	9.0.0.21	10.17.41.16	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5551
3744	CVE-2017-15289	Low	Medium	The mode4and5 write functions in hw/display/cirrus_vga.c in Qemu allow local OS guest privileged users to cause a denial of service (out-of-bounds write access and Qemu process crash) via vectors related to dst calculation.	qemu	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5706
3745	CVE-2017-15286	MEDIUM	High	SQLite 3.20.1 has a NULL pointer dereference in tableColumnList in shell.c because it fails to consider certain cases where `sqlite3_step(pStmt)==SQLITE_ROW` is false and a data structure is never initialized.	sqlite	Unchanged	Won't Fix	Won't Fix	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5561
3746	CVE-2017-15281	MEDIUM	High	ReadPSDImage in coders/psd.c in ImageMagick 7.0.7-6 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to Conditional jump or move depends on uninitialised value(s).	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5580
3747	CVE-2017-15277	MEDIUM	Medium	ReadGIFImage in coders/gif.c in ImageMagick 7.0.6-1 and GraphicsMagick 1.3.26 leaves the palette uninitialized when processing a GIF file that has neither a global nor local palette. If the affected product is used as a library loaded into a process that operates on interesting data, this data sometimes can be leaked via the uninitialized palette.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5532
3748	CVE-2017-15275	MEDIUM	High	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear allocated heap memory.	samba	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2615
3749	CVE-2017-15274	MEDIUM	Medium	security/keys/keyctl.c in the Linux kernel before 4.11.5 does not consider the case of a NULL payload in conjunction with a nonzero length value, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted add_key or keyctl system call, a different vulnerability than CVE-2017-12192.	linux	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5521

	A	B	C	D	E	F	G	H	I	J	K	L	M
3750	CVE-2017-15268	MEDIUM	High	Qemu through 2.10.0 allows remote attackers to cause a memory leak by triggering slow data-channel read operations, related to io/channel-websock.c.	qemu	Unchanged	Not vulnerable	9.0.0.12	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5537
3751	CVE-2017-15265	Medium	High	Race condition in the ALSA subsystem in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted /dev/snd/seq ioctl calls, related to sound/core/seq/seq_clientmgr.c and sound/core/seq/seq_ports.c.	linux	Unchanged	8.0.0.23	9.0.0.12	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5687
3752	CVE-2017-15232	MEDIUM	Medium	libjpeg-turbo 1.5.2 has a NULL Pointer Dereference in jdpostct.c and jquant1.c via a crafted JPEG file.	libjpeg-turbo	Unchanged	Won't Fix	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-5603
3753	CVE-2017-15228	Medium	High	Irssi before 1.0.5, when installing themes with unterminated colour formatting sequences, may access data beyond the end of the string.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5698
3754	CVE-2017-15227	Medium	High	Irssi before 1.0.5, while waiting for the channel synchronisation, may incorrectly fail to remove destroyed channels from the query list, resulting in use-after-free conditions when updating the state later on.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5688
3755	CVE-2017-15225	MEDIUM	Medium	_bfd_dwarf2_cleanup_debug_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (memory leak) via a crafted ELF file.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5566
3756	CVE-2017-15218	MEDIUM	Medium	ImageMagick 7.0.7-2 has a memory leak in ReadOneJNGImage in coders/png.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5593
3757	CVE-2017-15217	MEDIUM	Medium	ImageMagick 7.0.7-2 has a memory leak in ReadSGIImage in coders/sgi.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5515
3758	CVE-2017-15193	HIGH	High	In Wireshark 2.4.0 to 2.4.1 and 2.2.0 to 2.2.9, the MBIM dissector could crash or exhaust system memory. This was addressed in epan/dissectors/packet-mbim.c by changing the memory-allocation approach.	wireshark	Unchanged	Not vulnerable	9.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5592
3759	CVE-2017-15192	MEDIUM	High	In Wireshark 2.4.0 to 2.4.1 and 2.2.0 to 2.2.9, the BT ATT dissector could crash. This was addressed in epan/dissectors/packet-btatt.c by considering a case where not all of the BTATT packets have the same encapsulation level.	wireshark	Unchanged	Not vulnerable	9.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5584
3760	CVE-2017-15191	MEDIUM	High	In Wireshark 2.4.0 to 2.4.1, 2.2.0 to 2.2.9, and 2.0.0 to 2.0.15, the DMP dissector could crash. This was addressed in epan/dissectors/packet-dmp.c by validating a string length.	wireshark	Unchanged	8.0.0.28	9.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5606
3761	CVE-2017-15190	MEDIUM	High	In Wireshark 2.4.0 to 2.4.1, the RTSP dissector could crash. This was addressed in epan/dissectors/packet-rtsp.c by correcting the scope of a variable.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5523
3762	CVE-2017-15189	MEDIUM	High	In Wireshark 2.4.0 to 2.4.1, the DOCSIS dissector could go into an infinite loop. This was addressed in plugins/docsis/packet-docsis.c by adding decrements.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5539
3763	CVE-2017-15186	MEDIUM	Medium	Double free vulnerability in FFmpeg 3.3.4 and earlier allows remote attackers to cause a denial of service via a crafted AVI file.	ffmpeg	Unchanged	Not vulnerable	9.0.0.14	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5721
3764	CVE-2017-15132	MEDIUM	High	A flaw was found in dovecot 2.0 up to 2.2.33 and 2.3.0. An abort of SASL authentication results in a memory leak in dovecot's auth client used by login processes. The leak has impact in high performance configuration where same login processes are reused and can cause the process to crash due to memory exhaustion.	dovecot	Unchanged	8.0.0.25	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3191
3765	CVE-2017-15130	MEDIUM	MEDIUM	A denial of service flaw was found in dovecot before 2.2.34. An attacker able to generate random SNI server names could exploit TLS SNI configuration lookups, leading to excessive memory usage and the process to restart.	dovecot	Unchanged	8.0.0.26	9.0.0.16	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3566
3766	CVE-2017-15129	MEDIUM	Medium	A use-after-free vulnerability was found in network namespaces code affecting the Linux kernel before 4.14.11. The function get_net_ns_by_id() in net/core/net_namespace.c does not check for the net::count value after it has found a peer network in netns_ids idr, which could lead to double free and memory corruption. This vulnerability could allow an unprivileged local user to induce kernel memory corruption on the system, leading to a crash. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although it is thought to be unlikely.	linux	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3061
3767	CVE-2017-15128	MEDIUM	Medium	A flaw was found in the hugetlb_mcopy_atomic_pte function in mm/hugetlb.c in the Linux kernel before 4.13.12. A lack of size check could cause a denial of service (BUG).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3079
3768	CVE-2017-15127	MEDIUM	Medium	A flaw was found in the hugetlb_mcopy_atomic_pte function in mm/hugetlb.c in the Linux kernel before 4.13. A superfluous implicit page unlock for VM_SHARED hugetlbfs mapping could trigger a local denial of service (BUG).	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3075
3769	CVE-2017-15126	HIGH	High	A use-after-free flaw was found in fs/userfaultfd.c in the Linux kernel before 4.13.6. The issue is related to the handling of fork failure when dealing with event messages. Failure to fork correctly can lead to a situation where a fork event will be removed from an already freed list of events with userfaultfd_ctx_put().	linux	Unchanged	Not vulnerable	Not vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3064
3770	CVE-2017-15124	HIGH	High	VNC server implementation in Quick Emulator (QEMU) before 2.14.3 was found to be vulnerable to an unbounded memory allocation issue, as it did not throttle the framebuffer updates sent to its client. If the client did not consume these updates, VNC server allocates growing memory to hold onto this data. A malicious remote VNC client could use this flaw to cause DoS to the server host.	qemu	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3104
3771	CVE-2017-15119	MEDIUM	HIGH	Quick Emulator(Qemu) built with the Network Block Device(NBD) server support is vulnerable to a denial-of-service issue. It could occur if a client sent large option requests, making server waste CPU time on reading up to 4G bytes.	qemu	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4230
3772	CVE-2017-15118	HIGH	CRITICAL	A stack-based buffer overflow vulnerability was found in NBD server implementation in qemu allowing client to request an export name of size up to 4096 bytes, which in fact should be limited to 256 bytes, allowing to cause out-of-bounds stack write in qemu process.	qemu	Unchanged	Not vulnerable	Not vulnerable	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4196

	A	B	C	D	E	F	G	H	I	J	K	L	M
3773	CVE-2017-15116	MEDIUM	Medium	The rngapi_reset function in crypto/rng.c in the Linux kernel before 4.2 allows attackers to cause a denial of service (NULL pointer dereference).	linux	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2675
3774	CVE-2017-15115	HIGH	High	The sctp_do_peeloff function in net/sctp/socket.c in the Linux kernel before 4.14 does not check whether the intended netns is used in a peel-off action, which allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via crafted system calls.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2584
3775	CVE-2017-15107	MEDIUM	High	A vulnerability was found in the implementation of DNSSEC in Dnsmasq up to and including 2.78. Wildcard synthesized NSEC records could be improperly interpreted to prove the non-existence of hostnames that actually exist.	dnsmasq	Updated	8.0.0.25	9.0.0.25	10.17.41.20	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3216
3776	CVE-2017-15102	MEDIUM	Medium	The tower_probe function in drivers/usb/misc/legousbtower.c in the Linux kernel before 4.8.1 allows local users (who are physically proximate for inserting a crafted USB device) to gain privileges by leveraging a write-what-where condition that occurs after a race condition and a NULL pointer dereference.	linux	Unchanged	8.0.0.24	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2583
3777	CVE-2017-15099	MEDIUM	Medium	INSERT ... ON CONFLICT DO UPDATE commands in PostgreSQL 10.x before 10.1, 9.6.x before 9.6.6, and 9.5.x before 9.5.10 disclose table contents that the invoker lacks privilege to read. These exploits affect only tables where the attacker lacks full read access but has both INSERT and UPDATE privileges. Exploits bypass row level security policies and lack of SELECT privilege.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2668
3778	CVE-2017-15098	MEDIUM	High	Invalid json_populate_recordset or jsonb_populate_recordset function calls in PostgreSQL 10.x before 10.1, 9.6.x before 9.6.6, 9.5.x before 9.5.10, 9.4.x before 9.4.15, and 9.3.x before 9.3.20 can crash the server or disclose a few bytes of server memory.	postgresql	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2625
3779	CVE-2017-15096	LOW	Low	A flaw was found in GlusterFS in versions prior to 3.10. A null pointer dereference in send_brick_req function in glusterfsd/src/gf_attach.c may be used to cause denial of service.	glusterfs	Unchanged	Not vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5680
3780	CVE-2017-15088	HIGH	Critical	plugins/preauth/pkinit/pkinit_crypto_openssl.c in MIT Kerberos 5 (aka krb5) through 1.15.2 mishandles Distinguished Name (DN) fields, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) in situations involving untrusted X.509 data, related to the get_matching_data and X509_NAME_oneline_ex functions. NOTE: this has security relevance only in use cases outside of the MIT Kerberos distribution, e.g., the use of get_matching_data in KDC certauth plugin code that is specific to Red Hat.	krb5	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2607
3781	CVE-2017-15047	HIGH	Critical	The clusterLoadConfig function in cluster.c in Redis 4.0.2 allows attackers to cause a denial of service (out-of-bounds array index and application crash) or possibly have unspecified other impact by leveraging limited access to the machine.	redis	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5601
3782	CVE-2017-15046	MEDIUM	Medium	LAME 3.99.5 has a stack-based buffer overflow in unpack_read_samples in frontend/get_audio.c, a different vulnerability than CVE-2017-9412.	lame	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5582
3783	CVE-2017-15045	MEDIUM	Medium	LAME 3.99.5 has a heap-based buffer over-read in fill_buffer in libmp3lame/util.c, related to lame_encode_buffer_sample_t in libmp3lame/lame.c, a different vulnerability than CVE-2017-9410.	lame	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5559
3784	CVE-2017-15042	MEDIUM	Medium	An unintended cleartext issue exists in Go before 1.8.4 and 1.9.x before 1.9.1. RFC 4954 requires that, during SMTP, the PLAIN auth scheme must only be used on network connections secured with TLS. The original implementation of smtp.PlainAuth in Go 1.0 enforced this requirement, and it was documented to do so. In 2013, upstream issue #5184, this was changed so that the server may decide whether PLAIN is acceptable. The result is that if you set up a man-in-the-middle SMTP server that doesn't advertise STARTTLS and does advertise that PLAIN auth is OK, the smtp.PlainAuth implementation sends the username and password.	go	Unchanged	Not vulnerable	Won't Fix	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5549
3785	CVE-2017-15041	HIGH	Critical	Go before 1.8.4 and 1.9.x before 1.9.1 allows go get remote command execution. Using custom domains, it is possible to arrange things so that example.com/pkg1 points to a Subversion repository but example.com/pkg1/pkg2 points to a Git repository. If the Subversion repository includes a Git checkout in its pkg2 directory and some other work is done to ensure the proper ordering of operations, go get can be tricked into reusing this Git checkout for the fetch of code from pkg2. If the Subversion repository's Git checkout has malicious commands in .git/hooks/, they will execute on the system running go get.	go	Unchanged	Not vulnerable	Won't Fix	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5538
3786	CVE-2017-15038	LOW	Medium	Race condition in the v9fs_xattrwalk function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS users to obtain sensitive information from host heap memory via vectors related to reading extended attributes.	qemu	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5524
3787	CVE-2017-15033	MEDIUM	High	ImageMagick version 7.0.7-2 contains a memory leak in ReadYUVImage in coders/yuv.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5527
3788	CVE-2017-15032	HIGH	Critical	ImageMagick version 7.0.7-2 contains a memory leak in ReadYCBCRImage in coders/ycbcr.c.	imagemagick	Unchanged	Not vulnerable	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5558
3789	CVE-2017-15025	MEDIUM	Medium	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted ELF file.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5530
3790	CVE-2017-15024	MEDIUM	Medium	find_abstract_instance_name in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite recursion and application crash) via a crafted ELF file.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5589

	A	B	C	D	E	F	G	H	I	J	K	L	M
3791	CVE-2017-15023	MEDIUM	Medium	read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not properly validate the format count, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to concat_filename.	binutils	Unchanged	Not vulnerable	Not vulnerable	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5543
3792	CVE-2017-15022	MEDIUM	Medium	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not validate the DW_AT_name data type, which allows remote attackers to cause a denial of service (bfd_hash_hash NULL pointer dereference, or out-of-bounds access, and application crash) via a crafted ELF file, related to scan_unit_for_symbols and parse_comp_unit.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5605
3793	CVE-2017-15021	MEDIUM	Medium	bfd_get_debug_link_info_1 in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to bfd_getl32.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.8	Vulnerable	Vulnerable	Vulnerable	LIN9-5598
3794	CVE-2017-15020	MEDIUM	High	dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles pointers, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file, related to parse_die and parse_line_table, as demonstrated by a parse_die heap-based buffer over-read.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.8	Vulnerable	Vulnerable	Vulnerable	LIN9-5583
3795	CVE-2017-15019	MEDIUM	High	LAME 3.99.5 has a NULL Pointer Dereference in the hip_decode_init function within libmp3lame/mpglib_interface.c via a malformed mpg file, because of an incorrect calloc call.	lame	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5570
3796	CVE-2017-15018	MEDIUM	Medium	LAME 3.99.5 has a heap-based buffer over-read when handling a malformed file in k_34_4 in vbrquantize.c.	lame	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5562
3797	CVE-2017-15017	HIGH	Critical	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadOneMNGImage in coders/png.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5547
3798	CVE-2017-15016	HIGH	Critical	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadEnhMetaFile in coders/emf.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5573
3799	CVE-2017-15015	HIGH	Critical	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in PDFDelegateMessage in coders/pdf.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5550
3800	CVE-2017-14991	LOW	Medium	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel before 4.13.4 allows local users to obtain sensitive information from uninitialized kernel heap-memory locations via an SG_GET_REQUEST_TABLE ioctl call for /dev/sg0.	linux	Unchanged	8.0.0.23	9.0.0.12	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5517
3801	CVE-2017-14989	MEDIUM	Medium	A use-after-free in RenderFreetype in MagickCore/annotate.c in ImageMagick 7.0.7-4 Q16 allows attackers to crash the application via a crafted font file, because the FT_Done_Glyph function (from FreeType 2) is called at an incorrect place in the ImageMagick code.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5541
3802	CVE-2017-14977	Medium	High	The FoFiTrueType::getCFFBlock function in FoFiTrueType.cc in Poppler 0.59.0 has a NULL pointer dereference vulnerability due to lack of validation of a table pointer, which allows an attacker to launch a denial of service attack.	poppler	Unchanged	Won't Fix	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5572
3803	CVE-2017-14976	Medium	High	The FoFiType1C::convertToType0 function in FoFiType1C.cc in Poppler 0.59.0 has a heap-based buffer over-read vulnerability if an out-of-bounds font dictionary index is encountered, which allows an attacker to launch a denial of service attack.	poppler	Unchanged	Won't Fix	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5569
3804	CVE-2017-14975	Medium	High	The FoFiType1C::convertToType0 function in FoFiType1C.cc in Poppler 0.59.0 has a NULL pointer dereference vulnerability because a data structure is not initialized, which allows an attacker to launch a denial of service attack.	poppler	Unchanged	Won't Fix	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5516
3805	CVE-2017-14974	Medium	Medium	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandle the failure of a certain canonicalization step, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.	binutils	Unchanged	Not vulnerable	Not vulnerable	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5564
3806	CVE-2017-14970	Medium	High	In lib/ofp-util.c in Open vSwitch (OvS) before 2.8.1, there are multiple memory leaks while parsing malformed OpenFlow group mod messages. NOTE: the vendor disputes the relevance of this report, stating it can only be triggered by an OpenFlow controller, but OpenFlow controllers have much more direct and powerful ways to force Open vSwitch to allocate memory, such as by inserting flows into the flow table.	openvswitch	Unchanged	8.0.0.24	9.0.0.13	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5587
3807	CVE-2017-14954	Low	Medium	The waitid implementation in kernel/exit.c in the Linux kernel through 4.13.4 accesses rusage data structures in unintended cases, which allows local users to obtain sensitive information, and bypass the KASLR protection mechanism, via a crafted system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5525
3808	CVE-2017-14952	HIGH	Critical	Double free in i18n/zonemeta.cpp in International Components for Unicode (ICU) for C/C++ through 59.1 allows remote attackers to execute arbitrary code via a crafted string, aka a redundant UVector entry clean up function call issue.	icu	Unchanged	8.0.0.24	9.0.0.13	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5701
3809	CVE-2017-14940	Medium	Medium	scan_unit_for_symbols in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5581
3810	CVE-2017-14939	Medium	Medium	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles a length calculation, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to read_1_byte.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5535

	A	B	C	D	E	F	G	H	I	J	K	L	M
3811	CVE-2017-14938	Medium	Medium	_bfd_elf_slurp_version_tables in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted ELF file.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5567
3812	CVE-2017-14934	Medium	Medium	process_debug_info in dwarf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file that contains a negative size value in a CU structure.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5540
3813	CVE-2017-14933	Medium	Medium	read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file.	binutils	Unchanged	Not vulnerable	Not vulnerable	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5594
3814	CVE-2017-14932	Medium	Medium	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite loop) via a crafted ELF file.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5546
3815	CVE-2017-14930	High	Medium	Memory leak in decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5529
3816	CVE-2017-14929	Medium	High	In Poppler 0.59.0, memory corruption occurs in a call to Object::dictLookup() in Object.h after a repeating series of Gfx::display, Gfx::go, Gfx::execOp, Gfx::opFill, Gfx::doPatternFill, Gfx::doTilingPatternFill and Gfx::drawForm calls (aka a Gfx.cc infinite loop), a different vulnerability than CVE-2017-14519.	poppler	Unchanged	Won't Fix	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5600
3817	CVE-2017-14928	Medium	Medium	In Poppler 0.59.0, a NULL Pointer Dereference exists in AnnotRichMedia::Configuration::Configuration in Annot.cc via a crafted PDF document.	poppler	Unchanged	Won't Fix	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5536
3818	CVE-2017-14927	Medium	Medium	In Poppler 0.59.0, a NULL Pointer Dereference exists in the SplashOutputDev::type3D0() function in SplashOutputDev.cc via a crafted PDF document.	poppler	Unchanged	Won't Fix	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5568
3819	CVE-2017-14926	Medium	Medium	In Poppler 0.59.0, a NULL Pointer Dereference exists in AnnotRichMedia::Content::Content in Annot.cc via a crafted PDF document.	poppler	Unchanged	Won't Fix	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5579
3820	CVE-2017-14867	HIGH	High	Git before 2.10.5, 2.11.x before 2.11.4, 2.12.x before 2.12.5, 2.13.x before 2.13.6, and 2.14.x before 2.14.2 uses unsafe Perl scripts to support subcommands such as cvsserver, which allows attackers to execute arbitrary OS commands via shell metacharacters in a module name. The vulnerable code is reachable via git-shell even without CVS support.	git	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5560
3821	CVE-2017-14767	Medium	High	The sdp_parse_fmtp_config_h264 function in libavformat/rtpdec_h264.c in FFmpeg before 3.3.4 mishandles empty sprop-parameter-sets values, which allows remote attackers to cause a denial of service (heap buffer overflow) or possibly have unspecified other impact via a crafted sdp file.	ffmpeg	Unchanged	Not vulnerable	9.0.0.12	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5602
3822	CVE-2017-14746	HIGH	Critical	Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a crafted SMB1 request.	samba	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2624
3823	CVE-2017-14745	Medium	High	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, interpret a -1 value as a sorting count instead of an error flag, which allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.	binutils	Unchanged	Not vulnerable	Not vulnerable	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5604
3824	CVE-2017-14741	MEDIUM	Medium	The ReadCAPTIONImage function in coders/caption.c in ImageMagick 7.0.7-3 allows remote attackers to cause a denial of service (infinite loop) via a crafted font file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5452
3825	CVE-2017-14739	MEDIUM	High	The AcquireResampleFilterThreadSet function in magick/resample-private.h in ImageMagick 7.0.7-4 mishandles failed memory allocation, which allows remote attackers to cause a denial of service (NULL Pointer Dereference in DistortImage in MagickCore/distort.c, and application crash) via unspecified vectors.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5456
3826	CVE-2017-14729	MEDIUM	High	The *_get_synthetic_symtab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, do not ensure a unique PLT entry for a symbol, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c.	binutils	Unchanged	Not vulnerable	Not vulnerable	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5445
3827	CVE-2017-14696	MEDIUM	High	SaltStack Salt before 2016.3.8, 2016.11.x before 2016.11.8, and 2017.7.x before 2017.7.2 allows remote attackers to cause a denial of service via a crafted authentication request.	salt	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5704
3828	CVE-2017-14695	HIGH	Critical	Directory traversal vulnerability in minion id validation in SaltStack Salt before 2016.3.8, 2016.11.x before 2016.11.8, and 2017.7.x before 2017.7.2 allows remote minions with incorrect credentials to authenticate to a master via a crafted minion ID. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-12791.	salt	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5696
3829	CVE-2017-14684	HIGH	Medium	In ImageMagick 7.0.7-4 Q16, a memory leak vulnerability was found in the function ReadVIPSImage in coders/vips.c, which allows attackers to cause a denial of service (memory consumption in ResizeMagickMemory in MagickCore/memory.c) via a crafted file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5432
3830	CVE-2017-14682	MEDIUM	High	GetNextToken in MagickCore/token.c in ImageMagick 7.0.6 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted SVG document, a different vulnerability than CVE-2017-10928.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5468

	A	B	C	D	E	F	G	H	I	J	K	L	M
3831	CVE-2017-14634	MEDIUM	Medium	In libsndfile 1.0.28, a divide-by-zero error exists in the function double64_init() in double64.c, which may lead to DoS when playing a crafted audio file.	libsndfile	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-5448
3832	CVE-2017-14633	MEDIUM	Medium	In Xiph.Org libvorbis 1.3.5, an out-of-bounds array read vulnerability exists in the function mapping0_forward() in mapping0.c, which may lead to DoS when operating on a crafted audio file with vorbis_analysis().	libvorbis	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5449
3833	CVE-2017-14632	HIGH	Critical	Xiph.Org libvorbis 1.3.5 allows Remote Code Execution upon freeing uninitialized memory in the function vorbis_analysis_headerout() in info.c when vi->channels<=0, a similar issue to Mozilla bug 550184.	libvorbis	Unchanged	8.0.0.25	9.0.0.14	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5442
3834	CVE-2017-14626	HIGH	Critical	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_decode in coders/sixel.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5463
3835	CVE-2017-14625	HIGH	Critical	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_output_create in coders/sixel.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5457
3836	CVE-2017-14624	HIGH	Critical	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function PostscriptDelegateMessage in coders/ps.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5473
3837	CVE-2017-14617	MEDIUM	High	In Poppler 0.59.0, a floating point exception occurs in the ImageStream class in Stream.cc, which may lead to a potential attack when handling malicious PDF files.	poppler	Unchanged	Won't Fix	9.0.0.11	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5467
3838	CVE-2017-14607	MEDIUM	High	In ImageMagick 7.0.7-4 Q16, an out of bounds read flaw related to ReadTIFFImage has been reported in coders/tiff.c. An attacker could possibly exploit this flaw to disclose potentially sensitive memory or cause an application crash.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5446
3839	CVE-2017-14604	MEDIUM	Medium	GNOME Nautilus before 3.23.90 allows attackers to spoof a file type by using the .desktop file extension, as demonstrated by an attack in which a .desktop file's Name field ends in .pdf but this file's Exec field launches a malicious sh -c command. In other words, Nautilus provides no UI indication that a file actually has the potentially unsafe .desktop extension; instead, the UI only shows the .pdf extension. One (slightly) mitigating factor is that an attack requires the .desktop file to have execute permission. The solution is to ask the user to confirm that the file is supposed to be treated as a .desktop file, and then remember the user's answer in the metadata::trusted field.	nautilus	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5472
3840	CVE-2017-14533	Medium	Medium	ImageMagick 7.0.6-6 has a memory leak in ReadMATImage in coders/mat.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5441
3841	CVE-2017-14532	High	Critical	ImageMagick 7.0.7-0 has a NULL Pointer Dereference in TIFFIgnoreTags in coders/tiff.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5465
3842	CVE-2017-14531	High	Medium	ImageMagick 7.0.7-0 has a memory exhaustion issue in ReadSUNImage in coders/sun.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5455
3843	CVE-2017-14529	Medium	Medium	The pe_print_idata function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles HintName vector entries, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted PE file, related to the bfd_getl16 function.	binutils	Unchanged	8.0.0.25	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5464
3844	CVE-2017-14528	Medium	Medium	The TIFFSetProfiles function in coders/tiff.c in ImageMagick 7.0.6 has incorrect expectations about whether LibTIFF TIFFGetField return values imply that data validation has occurred, which allows remote attackers to cause a denial of service (use-after-free after an invalid call to TIFFSetField, and application crash) via a crafted file.	imagemagick	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5469
3845	CVE-2017-14520	Medium	High	In Poppler 0.59.0, a floating point exception occurs in Splash::scaleImageYuXd() in Splash.cc, which may lead to a potential attack when handling malicious PDF files.	poppler	Unchanged	Won't Fix	9.0.0.11	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5427
3846	CVE-2017-14519	Medium	High	In Poppler 0.59.0, memory corruption occurs in a call to Object::streamGetChar in Object.h after a repeating series of Gfx::display, Gfx::go, Gfx::execOp, Gfx::opShowText, and Gfx::doShowText calls (aka a Gfx.cc infinite loop).	poppler	Unchanged	Won't Fix	9.0.0.11	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5460
3847	CVE-2017-14518	Medium	High	In Poppler 0.59.0, a floating point exception exists in the isImageInterpolationRequired() function in Splash.cc via a crafted PDF document.	poppler	Unchanged	Won't Fix	9.0.0.11	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5461
3848	CVE-2017-14517	Medium	Medium	In Poppler 0.59.0, a NULL Pointer Dereference exists in the XRef::parseEntry() function in XRef.cc via a crafted PDF document.	poppler	Unchanged	Won't Fix	9.0.0.11	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5450
3849	CVE-2017-14505	Medium	Medium	DrawGetStrokeDashArray in wand/drawing-wand.c in ImageMagick 7.0.7-1 mishandles certain NULL arrays, which allows attackers to perform Denial of Service (NULL pointer dereference and application crash in AcquireQuantumMemory within MagickCore/memory.c) by providing a crafted Image File as input.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5453
3850	CVE-2017-14503	Medium	Medium	libarchive 3.3.2 suffers from an out-of-bounds read within lha_read_data_none() in archive_read_support_format_lha.c when extracting a specially crafted lha archive, related to lha_crc16.	libarchive	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5426
3851	CVE-2017-14502	Medium	High	read_header in archive_read_support_format_rar.c in libarchive 3.3.2 suffers from an off-by-one error for UTF-16 names in RAR archives, leading to an out-of-bounds read in archive_read_format_rar_read_header.	libarchive	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5429
3852	CVE-2017-14501	Medium	Medium	An out-of-bounds read flaw exists in parse_file_info in archive_read_support_format_iso9660.c in libarchive 3.3.2 when extracting a specially crafted iso9660 iso file, related to archive_read_format_iso9660_read_header.	libarchive	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5451
3853	CVE-2017-14497	High	High	The tpacket_rcv function in net/packet/af_packet.c in the Linux kernel before 4.13 mishandles vnet headers, which might allow local users to cause a denial of service (buffer overflow, and disk and memory corruption) or possibly have unspecified other impact via crafted system calls.	linux	Unchanged	Not vulnerable	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5462

	A	B	C	D	E	F	G	H	I	J	K	L	M
3854	CVE-2017-14496	HIGH	High	Integer underflow in the add_pseudoheader function in dnsmasq before 2.78 , when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service via a crafted DNS request.	dnsmasq	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5502
3855	CVE-2017-14495	MEDIUM	High	Memory leak in dnsmasq before 2.78, when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service (memory consumption) via vectors involving DNS response creation.	dnsmasq	Unchanged	Not vulnerable	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5501
3856	CVE-2017-14494	MEDIUM	Medium	dnsmasq before 2.78, when configured as a relay, allows remote attackers to obtain sensitive memory information via vectors involving handling DHCPv6 forwarded requests.	dnsmasq	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5500
3857	CVE-2017-14493	HIGH	Critical	Stack-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DHCPv6 request.	dnsmasq	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5499
3858	CVE-2017-14492	HIGH	Critical	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted IPv6 router advertisement request.	dnsmasq	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5498
3859	CVE-2017-14491	HIGH	Critical	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.	dnsmasq	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5497
3860	CVE-2017-14489	Medium	Medium	The iscsi_if_rx function in drivers/scsi/scsi_transport_iscsi.c in the Linux kernel through 4.13.2 allows local users to cause a denial of service (panic) by leveraging incorrect length validation.	linux	Unchanged	8.0.0.23	9.0.0.11	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5438
3861	CVE-2017-14482	MEDIUM	High	GNU Emacs before 25.3 allows remote attackers to execute arbitrary code via email with crafted Content-Type: text/enriched data containing an x-display XML element that specifies execution of shell commands, related to an unsafe text/enriched extension in lisp/textmodes/enriched.el, and unsafe Gnus support for enriched and richtext inline MIME objects in lisp/gnus/mm-view.el. In particular, an Emacs user can be instantly compromised by reading a crafted email message (or Usenet news article).	emacs	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5444
3862	CVE-2017-14461	MEDIUM	HIGH	A specially crafted email delivered over SMTP and passed on to Dovecot by MTA can trigger an out of bounds read resulting in potential sensitive information disclosure and denial of service. In order to trigger this vulnerability, an attacker needs to send a specially crafted email message to the server.	dovecot	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3529
3863	CVE-2017-14400	MEDIUM	Medium	In ImageMagick 7.0.7-1 Q16, the PersistPixelCache function in magick/cache.c mishandles the pixel cache nexus, which allows remote attackers to cause a denial of service (NULL pointer dereference in the function GetVirtualPixels in MagickCore/cache.c) via a crafted file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5347
3864	CVE-2017-14343	MEDIUM	Medium	ImageMagick 7.0.6-6 has a memory leak vulnerability in ReadXCFImage in coders/xcf.c via a crafted xcf image file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5395
3865	CVE-2017-14342	MEDIUM	Medium	ImageMagick 7.0.6-6 has a memory exhaustion vulnerability in ReadWPGImage in coders/wpg.c via a crafted wpg image file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5371
3866	CVE-2017-14341	HIGH	Medium	ImageMagick 7.0.6-6 has a large loop vulnerability in ReadWPGImage in coders/wpg.c, causing CPU exhaustion via a crafted wpg image file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5394
3867	CVE-2017-14340	MEDIUM	Medium	The XFS_IS_REALTIME_INODE macro in fs/xfs/xfs_linux.h in the Linux kernel before 4.13.2 does not verify that a filesystem has a realtime device, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via vectors related to setting an RHINHERIT flag on a directory.	linux	Unchanged	8.0.0.23	9.0.0.11	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5458
3868	CVE-2017-14333	MEDIUM	High	The process_version_sections function in readelf.c in GNU Binutils 2.29 allows attackers to cause a denial of service (Integer Overflow, and hang because of a time-consuming loop) or possibly have unspecified other impact via a crafted binary file with invalid values of ent.vn_next, during readelf -a execution.	binutils	Unchanged	8.0.0.25	9.0.0.14	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5377
3869	CVE-2017-14326	MEDIUM	Medium	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5298
3870	CVE-2017-14325	HIGH	Medium	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function PersistPixelCache in magick/cache.c, which allows attackers to cause a denial of service (memory consumption in ReadMPCImage in coders/mpc.c) via a crafted file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5210
3871	CVE-2017-14324	MEDIUM	Medium	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMPCImage in coders/mpc.c, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5263
3872	CVE-2017-14266	MEDIUM	High	tcprewrite in Tcpreplay 3.4.4 has a Heap-Based Buffer Overflow vulnerability triggered by a crafted PCAP file.	tcpreplay	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5305
3873	CVE-2017-14249	MEDIUM	Medium	ImageMagick 7.0.6-8 Q16 mishandles EOF checks in ReadMPCImage in coders/mpc.c, leading to division by zero in GetPixelCacheTileSize in MagickCore/cache.c, allowing remote attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5348
3874	CVE-2017-14248	MEDIUM	Medium	A heap-based buffer over-read in SampleImage() in MagickCore/resize.c in ImageMagick 7.0.6-8 Q16 allows remote attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	Not vulnerable	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5212
3875	CVE-2017-14246	MEDIUM	High	An out of bounds read in the function d2ulaw_array() in ulaw.c of libsndfile 1.0.28 may lead to a remote DoS attack or information disclosure, related to mishandling of the NAN and INFINITY floating-point values.	libsndfile	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5430
3876	CVE-2017-14245	MEDIUM	High	An out of bounds read in the function d2alaw_array() in alaw.c of libsndfile 1.0.28 may lead to a remote DoS attack or information disclosure, related to mishandling of the NAN and INFINITY floating-point values.	libsndfile	Unchanged	8.0.0.28	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5435

	A	B	C	D	E	F	G	H	I	J	K	L	M
3877	CVE-2017-14229	MEDIUM	High	There is an infinite loop in the jpc_dec_tileinit function in jpc/jpc_dec.c of Jasper 2.0.13. It will lead to a remote denial of service attack.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5254
3878	CVE-2017-14228	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, there is an illegal address access in the function paste_tokens() in preproc.c, aka a NULL pointer dereference. It will lead to remote denial of service.	nasm	Unchanged	8.0.0.23	9.0.0.12	10.17.41.3	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5246
3879	CVE-2017-14227	MEDIUM	High	In MongoDB libbson 1.7.0, the bson_iter_codewscope function in bson-iter.c miscalculates a bson_utf8_validate length argument, which allows remote attackers to cause a denial of service (heap-based buffer over-read in the bson_utf8_validate function in bson-utf8.c), as demonstrated by bson-to-json.c.	mongodb	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5345
3880	CVE-2017-14225	MEDIUM	High	The av_color_primaries_name function in libavutil/pixdesc.c in FFmpeg 3.3.3 may return a NULL pointer depending on a value contained in a file, but callers do not anticipate this, as demonstrated by the avcodec_string function in libavcodec/utils.c, leading to a NULL pointer dereference. (It is also conceivable that there is security relevance for a NULL pointer dereference in av_color_primaries_name calls within the ffprobe command-line program.)	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5383
3881	CVE-2017-14224	MEDIUM	High	A heap-based buffer overflow in WritePCXImage in coders/pcx.c in ImageMagick 7.0.6-8 Q16 allows remote attackers to cause a denial of service or code execution via a crafted file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5243
3882	CVE-2017-14223	HIGH	Medium	In libavformat/asfdec_f.c in FFmpeg 3.3.3, a DoS in asf_build_simple_index() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted ASF file, which claims a large ict field in the header but does not contain sufficient backing data, is provided, the for loop would consume huge CPU and memory resources, since there is no EOF check inside the loop.	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5301
3883	CVE-2017-14222	HIGH	Medium	In libavformat/mov.c in FFmpeg 3.3.3, a DoS in read_tfra() due to lack of an EOF (End of File) check might cause huge CPU and memory consumption. When a crafted MOV file, which claims a large item_count field in the header but does not contain sufficient backing data, is provided, the loop would consume huge CPU and memory resources, since there is no EOF check inside the loop.	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5349
3884	CVE-2017-14175	High	Medium	In coders/xbm.c in ImageMagick 7.0.6-1 Q16, a DoS in ReadXBMImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted XBM file, which claims large rows and columns fields in the header but does not contain sufficient backing data, is provided, the loop over the rows would consume huge CPU resources, since there is no EOF check inside the loop.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5247
3885	CVE-2017-14174	High	Medium	In coders/psd.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSDLayersInternal() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large length field in the header but does not contain sufficient backing data, is provided, the loop over length would consume huge CPU resources, since there is no EOF check inside the loop.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5252
3886	CVE-2017-14173	Medium	Medium	In the function ReadTXTImage() in coders/txt.c in ImageMagick 7.0.6-10, an integer overflow might occur for the addition operation GetQuantumRange(depth)+1 when depth is large, producing a smaller value than expected. As a result, an infinite loop would occur for a crafted TXT file that claims a very large max_value value.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5351
3887	CVE-2017-14172	High	Medium	In coders/ps.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large extent field in the header but does not contain sufficient backing data, is provided, the loop over length would consume huge CPU resources, since there is no EOF check inside the loop.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5325
3888	CVE-2017-14171	High	Medium	In libavformat/nsvdec.c in FFmpeg 3.3.3, a DoS in nsv_parse_NSVf_header() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted NSV file, which claims a large table_entries_used field in the header but does not contain sufficient backing data, is provided, the loop over 'table_entries_used' would consume huge CPU resources, since there is no EOF check inside the loop.	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5284
3889	CVE-2017-14170	High	Medium	In libavformat/mxfdec.c in FFmpeg 3.3.3, a DoS in mxf_read_index_entry_array() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted MXF file, which claims a large nb_index_entries field in the header but does not contain sufficient backing data, is provided, the loop would consume huge CPU resources, since there is no EOF check inside the loop. Moreover, this big loop can be invoked multiple times if there is more than one applicable data segment in the crafted MXF file.	ffmpeg	Unchanged	Not vulnerable	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5269
3890	CVE-2017-14169	Medium	High	In the mxf_read_primer_pack function in libavformat/mxfdec.c in FFmpeg 3.3.3, an integer signedness error might occur when a crafted file, which claims a large item_num field such as 0xffffffff, is provided. As a result, the variable item_num turns negative, bypassing the check for a large value.	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5363
3891	CVE-2017-14167	HIGH	High	Integer overflow in the load_multiboot function in hw/i386/multiboot.c in QEMU (aka Quick Emulator) allows local guest OS users to execute arbitrary code on the host via crafted multiboot header address values, which trigger an out-of-bounds write.	qemu	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5321

	A	B	C	D	E	F	G	H	I	J	K	L	M
3892	CVE-2017-14166	Medium	Medium	libarchive 3.3.2 allows remote attackers to cause a denial of service (xml_data heap-based buffer over-read and application crash) via a crafted xar archive, related to the mishandling of empty strings in the atol8 function in archive_read_support_format_xar.c.	libarchive	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5402
3893	CVE-2017-14164	MEDIUM	High	A size-validation issue was discovered in opj_j2k_write_sot in lib/openjp2/j2k.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service (heap-based buffer overflow affecting opj_write_bytes_LE in lib/openjp2/cio.c) or possibly remote code execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-14152.	openjpeg	Unchanged	Won't Fix	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5280
3894	CVE-2017-14160	MEDIUM	High	The bark_noise_hybridmp function in psy.c in Xiph.Org libvorbis 1.3.5 allows remote attackers to cause a denial of service (out-of-bounds access and application crash) or possibly have unspecified other impact via a crafted mp4 file.	libvorbis	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5443
3895	CVE-2017-14159	LOW	Medium	slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for PID file modification before a root script executes a kill `cat /pathname` command, as demonstrated by openldap-initscript.	openldap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5208
3896	CVE-2017-14156	Low	Medium	The atyfb_ioctl function in drivers/video/fbdev/aty/atyfb_base.c in the Linux kernel through 4.12.10 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading locations associated with padding bytes.	linux	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5262
3897	CVE-2017-14152	Medium	High	A mishandled zero case was discovered in opj_j2k_set_cinema_parameters in lib/openjp2/j2k.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service (heap-based buffer overflow affecting opj_write_bytes_LE in lib/openjp2/cio.c and opj_j2k_write_sot in lib/openjp2/j2k.c) or possibly remote code execution.	openjpeg	Unchanged	Won't Fix	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5303
3898	CVE-2017-14151	Medium	High	An off-by-one error was discovered in opj_tcd_code_block_enc_allocate_data in lib/openjp2/tcd.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service (heap-based buffer overflow affecting opj_mqc_flush in lib/openjp2/mqc.c and opj_t1_encode_cblk in lib/openjp2/t1.c) or possibly remote code execution.	openjpeg	Unchanged	Won't Fix	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5282
3899	CVE-2017-14140	Low	Medium	The move_pages system call in mm/migrate.c in the Linux kernel before 4.12.9 doesn't check the effective uid of the target process, enabling a local attacker to learn the memory layout of a setuid executable despite ASLR.	linux	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5304
3900	CVE-2017-14139	Medium	High	ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteMSLImage in coders/msl.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5379
3901	CVE-2017-14138	High	Critical	ImageMagick 7.0.6-5 has a memory leak vulnerability in ReadWEBPImage in coders/webp.c because memory is not freed in certain error cases, as demonstrated by VP8 errors.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5357
3902	CVE-2017-14137	High	Critical	ReadWEBPImage in coders/webp.c in ImageMagick 7.0.6-5 has an issue where memory allocation is excessive because it depends only on a length field in a header.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5240
3903	CVE-2017-14136	Medium	Medium	OpenCV (Open Source Computer Vision Library) 3.3 has an out-of-bounds write error in the function FillColorRow1 in utils.cpp when reading an image file by using cv::imread. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-12597.	opencv	Unchanged	Won't Fix	Investigate	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5229
3904	CVE-2017-14132	Medium	Medium	JasPer 2.0.13 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted image, related to the jas_image_ishomosamp function in libjasper/base/jas_image.c.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5401
3905	CVE-2017-14130	Medium	Medium	The _bfd_elf_parse_attributes function in elf-attrs.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (_bfd_elf_attr_strdup heap-based buffer over-read and application crash) via a crafted ELF file.	binutils	Unchanged	8.0.0.23	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5187
3906	CVE-2017-14129	Medium	Medium	The read_section function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (parse_comp_unit heap-based buffer over-read and application crash) via a crafted ELF file.	binutils	Unchanged	8.0.0.23	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5188
3907	CVE-2017-14128	Medium	Medium	The decode_line_info function in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (read_1_byte heap-based buffer over-read and application crash) via a crafted ELF file.	binutils	Unchanged	8.0.0.23	9.0.0.12	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5192
3908	CVE-2017-14108	High	Medium	libgedit.a in GNOME gedit through 3.22.1 allows remote attackers to cause a denial of service (CPU consumption) via a file that begins with many '\0' characters.	gedit	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5259
3909	CVE-2017-14107	Medium	Medium	The _zip_read_eocd64 function in zip_open.c in libzip before 1.3.0 mishandles EOCD records, which allows remote attackers to cause a denial of service (memory allocation failure in _zip_cdir_grow in zip_dirent.c) via a crafted ZIP archive.	php	Unchanged	8.0.0.27	9.0.0.17	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4168
3910	CVE-2017-14106	Medium	Medium	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp_recvmsg code path.	linux	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5191

	A	B	C	D	E	F	G	H	I	J	K	L	M
3911	CVE-2017-14064	HIGH	Critical	Ruby through 2.2.7, 2.3.x through 2.3.4, and 2.4.x through 2.4.1 can expose arbitrary memory during a JSON.generate call. The issues lies in using strdup in ext/json/ext/generator/generator.c, which will stop after encountering a \0' byte, returning a pointer to a string of length zero, which is not the length stored in space_len.	ruby	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5274
3912	CVE-2017-14060	Medium	Medium	In ImageMagick 7.0.6-10, a NULL Pointer Dereference issue is present in the ReadCUTImage function in coders/cut.c that could allow an attacker to cause a Denial of Service (in the QueueAuthenticPixelCacheNexus function within the MagickCore/cache.c file) by submitting a malformed image file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5266
3913	CVE-2017-14059	High	Medium	In FFmpeg 3.3.3, a DoS in cine_read_header() due to lack of an EOF check might cause huge CPU and memory consumption. When a crafted CINE file, which claims a large duration field in the header but does not contain sufficient backing data, is provided, the image-offset parsing loop would consume huge CPU and memory resources, since there is no EOF check inside the loop.	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5273
3914	CVE-2017-14058	Medium	Medium	In FFmpeg 3.3.3, the read_data function in libavformat/hls.c does not restrict reload attempts for an insufficient list, which allows remote attackers to cause a denial of service (infinite loop).	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5341
3915	CVE-2017-14057	High	Medium	In FFmpeg 3.3.3, a DoS in asf_read_marker() due to lack of an EOF (End of File) check might cause huge CPU and memory consumption. When a crafted ASF file, which claims a large name_len or count field in the header but does not contain sufficient backing data, is provided, the loops over the name and markers would consume huge CPU and memory resources, since there is no EOF check inside these loops.	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5386
3916	CVE-2017-14056	High	Medium	In libavformat/rl2.c in FFmpeg 3.3.3, a DoS in rl2_read_header() due to lack of an EOF (End of File) check might cause huge CPU and memory consumption. When a crafted RL2 file, which claims a large frame_count field in the header but does not contain sufficient backing data, is provided, the loops (for offset and size tables) would consume huge CPU and memory resources, since there is no EOF check inside these loops.	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5283
3917	CVE-2017-14055	High	Medium	In libavformat/mvdec.c in FFmpeg 3.3.3, a DoS in mv_read_header() due to lack of an EOF (End of File) check might cause huge CPU and memory consumption. When a crafted MV file, which claims a large nb_frames field in the header but does not contain sufficient backing data, is provided, the loop over the frames would consume huge CPU and memory resources, since there is no EOF check inside the loop.	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5225
3918	CVE-2017-14054	High	Medium	In libavformat/rmdec.c in FFmpeg 3.3.3, a DoS in ivr_read_header() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted IVR file, which claims a large len field in the header but does not contain sufficient backing data, is provided, the first type==4 loop would consume huge CPU resources, since there is no EOF check inside the loop.	ffmpeg	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5366
3919	CVE-2017-14051	Medium	Medium	An integer overflow in the qla2x00_sysfs_write_optrom_ctl function in drivers/scsi/qla2xxx/qla_attr.c in the Linux kernel through 4.12.10 allows local users to cause a denial of service (memory corruption and system crash) by leveraging root access.	linux	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5277
3920	CVE-2017-14041	Medium	High	A stack-based buffer overflow was discovered in the pgxtoimage function in bin/jp2/convert.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly remote code execution.	openjpeg	Unchanged	Won't Fix	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5393
3921	CVE-2017-14040	Medium	High	An invalid write access was discovered in bin/jp2/convert.c in OpenJPEG 2.2.0, triggering a crash in the tgatoimage function. The vulnerability may lead to remote denial of service or possibly unspecified other impact.	openjpeg	Unchanged	Won't Fix	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5233
3922	CVE-2017-14039	Medium	High	A heap-based buffer overflow was discovered in the opj_t2_encode_packet function in lib/openjp2/t2.c in OpenJPEG 2.2.0. The vulnerability causes an out-of-bounds write, which may lead to remote denial of service or possibly unspecified other impact.	openjpeg	Unchanged	Won't Fix	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5279
3923	CVE-2017-14033	MEDIUM	High	The decode method in the OpenSSL::ASN1 module in Ruby before 2.2.8, 2.3.x before 2.3.5, and 2.4.x through 2.4.1 allows attackers to cause a denial of service (interpreter crash) via a crafted string.	ruby	Unchanged	8.0.0.23	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5466
3924	CVE-2017-13768	Medium	Medium	Null Pointer Dereference in the IdentifyImage function in MagickCore/identify.c in ImageMagick through 7.0.6-10 allows an attacker to perform denial of service by sending a crafted image file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5335
3925	CVE-2017-13767	High	High	In Wireshark 2.4.0, 2.2.0 to 2.2.8, and 2.0.0 to 2.0.14, the MSDP dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-msdp.c by adding length validation.	wireshark	Unchanged	Not vulnerable	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5337
3926	CVE-2017-13766	Medium	High	In Wireshark 2.4.0 and 2.2.0 to 2.2.8, the Profinet I/O dissector could crash with an out-of-bounds write. This was addressed in plugins/profinet/packet-dcerpc-pn-io.c by adding string validation.	wireshark	Unchanged	Not vulnerable	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5292
3927	CVE-2017-13765	Medium	High	In Wireshark 2.4.0, 2.2.0 to 2.2.8, and 2.0.0 to 2.0.14, the IrCOMM dissector has a buffer over-read and application crash. This was addressed in plugins/irda/packet-ircomm.c by adding length validation.	wireshark	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5331
3928	CVE-2017-13764	Medium	High	In Wireshark 2.4.0, the Modbus dissector could crash with a NULL pointer dereference. This was addressed in epan/dissectors/packet-mbtcp.c by adding length validation.	wireshark	Unchanged	Not vulnerable	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5296
3929	CVE-2017-13758	Medium	Medium	In ImageMagick 7.0.6-10, there is a heap-based buffer overflow in the TracePoint() function in MagickCore/draw.c.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5293

	A	B	C	D	E	F	G	H	I	J	K	L	M
3930	CVE-2017-13757	Medium	Medium	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not validate the PLT section size, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to elf_i386_get_synthetic_symtab in elf32-i386.c and elf_x86_64_get_synthetic_symtab in elf64-x86-64.c.	binutils	Unchanged	Not vulnerable	Not vulnerable	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5237
3931	CVE-2017-13752	Medium	High	There is a reachable assertion abort in the function jpc_dequantize() in jpc/jpc_dec.c in JasPer 2.0.12 that will lead to a remote denial of service attack.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5272
3932	CVE-2017-13751	Medium	High	There is a reachable assertion abort in the function calcstepsizes() in jpc/jpc_dec.c in JasPer 2.0.12 that will lead to a remote denial of service attack.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5281
3933	CVE-2017-13750	Medium	High	There is a reachable assertion abort in the function jpc_dec_process_siz() in jpc/jpc_dec.c:1296 in JasPer 2.0.12 that will lead to a remote denial of service attack.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5353
3934	CVE-2017-13749	Medium	High	There is a reachable assertion abort in the function jpc_pi_nextrpcl() in jpc/jpc_t2cod.c in JasPer 2.0.12 that will lead to a remote denial of service attack.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5213
3935	CVE-2017-13748	Medium	High	There are lots of memory leaks in JasPer 2.0.12, triggered in the function jas_strdup() in base/jas_string.c, that will lead to a remote denial of service attack.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5387
3936	CVE-2017-13747	Medium	High	There is a reachable assertion abort in the function jpc_floorlog2() in jpc/jpc_math.c in JasPer 2.0.12 that will lead to a remote denial of service attack.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5354
3937	CVE-2017-13746	Medium	High	There is a reachable assertion abort in the function jpc_dec_process_siz() in jpc/jpc_dec.c:1297 in JasPer 2.0.12 that will lead to a remote denial of service attack.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5328
3938	CVE-2017-13745	Medium	High	There is a reachable assertion abort in the function jpc_dec_process_sot() in jpc/jpc_dec.c in JasPer 2.0.12 that will lead to a remote denial of service attack.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5244
3939	CVE-2017-13734	Medium	Medium	There is an illegal address access in the _nc_safe_strcat function in strings.c in ncurses 6.0 that will lead to a remote denial of service attack.	ncurses	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5322
3940	CVE-2017-13733	Medium	Medium	There is an illegal address access in the fmt_entry function in progs/dump_entry.c in ncurses 6.0 that might lead to a remote denial of service attack.	ncurses	Unchanged	8.0.0.25	9.0.0.14	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5330
3941	CVE-2017-13732	Medium	Medium	There is an illegal address access in the function dump_uses() in progs/dump_entry.c in ncurses 6.0 that might lead to a remote denial of service attack.	ncurses	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5338
3942	CVE-2017-13731	Medium	Medium	There is an illegal address access in the function postprocess_termcap() in parse_entry.c in ncurses 6.0 that will lead to a remote denial of service attack.	ncurses	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5205
3943	CVE-2017-13730	Medium	Medium	There is an illegal address access in the function _nc_read_entry_source() in progs/tic.c in ncurses 6.0 that might lead to a remote denial of service attack.	ncurses	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5276
3944	CVE-2017-13729	Medium	Medium	There is an illegal address access in the _nc_save_str function in alloc_entry.c in ncurses 6.0. It will lead to a remote denial of service attack.	ncurses	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5257
3945	CVE-2017-13728	Medium	High	There is an infinite loop in the next_char function in comp_scan.c in ncurses 6.0, related to libtic. A crafted input will lead to a remote denial of service attack.	ncurses	Unchanged	8.0.0.22	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5253
3946	CVE-2017-13727	Medium	Medium	There is a reachable assertion abort in the function TIFFWriteDirectoryTagSubifd() in LibTIFF 4.0.8, related to tif_dirwrite.c and a SubIFD tag. A crafted input will lead to a remote denial of service attack.	libtiff	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5332
3947	CVE-2017-13726	Medium	Medium	There is a reachable assertion abort in the function TIFFWriteDirectorySec() in LibTIFF 4.0.8, related to tif_dirwrite.c and a SubIFD tag. A crafted input will lead to a remote denial of service attack.	libtiff	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5209
3948	CVE-2017-13725	HIGH	Critical	The IPv6 routing header parser in tcpdump before 4.9.2 has a buffer over-read in print-rt6.c:rt6_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5260
3949	CVE-2017-13723	MEDIUM	High	In X.Org Server (aka xserver and xorg-server) before 1.19.4, a local attacker authenticated to the X server could overflow a global buffer, causing crashes of the X server or potentially other problems by injecting large or malformed XKB related atoms and accessing them via xkbcomp.	xorg	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5563
3950	CVE-2017-13722	LOW	High	In the pcfGetProperties function in bitmap/pcfread.c in libXfont through 1.5.2 and 2.x before 2.0.2, a missing boundary check (for PCF files) could be used by local attackers authenticated to an Xserver for a buffer over-read, for information disclosure or a crash of the X server.	libxfont	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5576
3951	CVE-2017-13721	LOW	Medium	In X.Org Server (aka xserver and xorg-server) before 1.19.4, an attacker authenticated to an X server with the X shared memory extension enabled can cause aborts of the X server or replace shared memory segments of other X clients in the same session.	xorg	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5556
3952	CVE-2017-13720	LOW	High	In the PatternMatch function in fontfile/fontdir.c in libXfont through 1.5.2 and 2.x before 2.0.2, an attacker with access to an X connection can cause a buffer over-read during pattern matching of fonts, leading to information disclosure or a crash (denial of service). This occurs because '\0' characters are incorrectly skipped in situations involving ? characters.	libxfont	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5545
3953	CVE-2017-13716	High	Medium	The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted file, as demonstrated by a call from the Binary File Descriptor (BFD) library (aka libbfd).	binutils	Unchanged	Investigate	Vulnerable	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5216

	A	B	C	D	E	F	G	H	I	J	K	L	M
3954	CVE-2017-13715	High	Critical	The __skb_flow_dissect function in net/core/flow_dissector.c in the Linux kernel before 4.3 does not ensure that n_proto, ip_proto, and thoff are initialized, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a single crafted MPLS packet.	linux	Unchanged	8.0.0.22	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5190
3955	CVE-2017-13712	Medium	High	NULL Pointer Dereference in the id3v2AddAudioDuration function in libmp3lame/id3tag.c in LAME 3.99.5 allows attackers to perform Denial of Service by triggering a NULL first argument.	lame	Unchanged	8.0.0.28	9.0.0.19	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5223
3956	CVE-2017-13711	Medium	High	Use-after-free vulnerability in the sofree function in slirp/socket.c in QEMU (aka Quick Emulator) allows attackers to cause a denial of service (QEMU instance crash) by leveraging failure to properly clear ifq_so from pending packets.	qemu	Unchanged	Not vulnerable	Not vulnerable	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5219
3957	CVE-2017-13710	MEDIUM	High	The setup_group function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a group section that is too small.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5161
3958	CVE-2017-13704	MEDIUM	High	In dnsmasq before 2.78, if the DNS packet size does not match the expected size, the size parameter in a memset call gets a negative value. As it is an unsigned value, memset ends up writing up to 0xffffffff zero's (0xffffffffffffffff in 64 bit platforms), making dnsmasq crash.	dnsmasq	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5506
3959	CVE-2017-13695	LOW	Medium	The acpi_ns_evaluate() function in drivers/acpi/acpica/nseval.c in the Linux kernel through 4.12.9 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.	linux	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5127
3960	CVE-2017-13694	LOW	Medium	The acpi_ps_complete_final_op() function in drivers/acpi/acpica/psobject.c in the Linux kernel through 4.12.9 does not flush the node and node_ext caches and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.	linux	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5138
3961	CVE-2017-13693	MEDIUM	Medium	The acpi_ds_create_operands() function in drivers/acpi/acpica/dsutils.c in the Linux kernel through 4.12.9 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.	linux	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5156
3962	CVE-2017-13690	HIGH	Critical	The IKEv2 parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5384
3963	CVE-2017-13689	HIGH	Critical	The IKEv1 parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c:ikev1_id_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5230
3964	CVE-2017-13688	HIGH	Critical	The OLSR parser in tcpdump before 4.9.2 has a buffer over-read in print-olsr.c:olsr_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5302
3965	CVE-2017-13687	HIGH	Critical	The Cisco HDLC parser in tcpdump before 4.9.2 has a buffer over-read in print-chdlc.c:chdlc_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5380
3966	CVE-2017-13686	HIGH	High	net/ipv4/route.c in the Linux kernel 4.13-rc1 through 4.13-rc6 is too late to check for a NULL fi field when RTM_F_FIB_MATCH is set, which allows local users to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via crafted system calls. NOTE: this does not affect any stable release.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5145
3967	CVE-2017-13685	Medium	Medium	The dump_callback function in SQLite 3.20.0 allows remote attackers to cause a denial of service (EXC_BAD_ACCESS and application crash) via a crafted file.	sqlite	Unchanged	8.0.0.30	9.0.0.21	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5255
3968	CVE-2017-13673	Medium	Medium	The vga display update in Qemu 2.8.0 through 2.9.0 mis-calculated the region for the dirty bitmap snapshot in case split screen mode is used causing a denial of service (assertion failure) in the cpu_physical_memory_snapshot_get_dirty function.	qemu	Unchanged	Not vulnerable	Not vulnerable	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5368
3969	CVE-2017-13672	Low	Medium	QEMU (aka Quick Emulator), when built with the VGA display emulator support, allows local guest OS privileged users to cause a denial of service (out-of-bounds read and QEMU process crash) via vectors involving display update.	qemu	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5391
3970	CVE-2017-13658	MEDIUM	Medium	In ImageMagick before 6.9.9-3 and 7.x before 7.0.6-3, there is a missing NULL check in the ReadMATImage function in coders/mat.c, leading to a denial of service (assertion failure and application exit) in the DestroyImageInfo function in MagickCore/image.c.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5135
3971	CVE-2017-13305	MEDIUM	MEDIUM	A information disclosure vulnerability in the Upstream kernel encrypted-keys. Product: Android. Versions: Android kernel. Android ID: A-70526974.	linux	Unchanged	8.0.0.31	9.0.0.22	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4334
3972	CVE-2017-13168	MEDIUM	High	An elevation of privilege vulnerability in the kernel scsi driver. Product: Android. Versions: Android kernel. Android ID A-65023233.	linux	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4335
3973	CVE-2017-13166	MEDIUM	High	An elevation of privilege vulnerability in the kernel v4l2 video driver. Product: Android. Versions: Android kernel. Android ID A-34624167.	linux	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4186
3974	CVE-2017-13146	MEDIUM	High	In ImageMagick before 6.9.8-5 and 7.x before 7.0.5-6, there is a memory leak in the ReadMATImage function in coders/mat.c.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5124
3975	CVE-2017-13145	MEDIUM	Medium	In ImageMagick before 6.9.8-8 and 7.x before 7.0.5-9, the ReadJP2Image function in coders/jp2.c does not properly validate the channel geometry, leading to a crash.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5125
3976	CVE-2017-13144	MEDIUM	Medium	In ImageMagick before 6.9.7-10, there is a crash (rather than a width or height exceeds limit error report) if the image dimensions are too large, as demonstrated by use of the mpc coder.	imagemagick	Unchanged	8.0.0.22	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5121

	A	B	C	D	E	F	G	H	I	J	K	L	M
3977	CVE-2017-13143	MEDIUM	High	In ImageMagick before 6.9.7-6 and 7.x before 7.0.4-6, the ReadMATImage function in coders/mat.c uses uninitialized data, which might allow remote attackers to obtain sensitive information from process memory.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5140
3978	CVE-2017-13142	MEDIUM	Medium	In ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1, a crafted PNG file could trigger a crash because there was an insufficient check for short files.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5147
3979	CVE-2017-13141	MEDIUM	Medium	In ImageMagick before 6.9.9-4 and 7.x before 7.0.6-4, a crafted file could trigger a memory leak in ReadOnePNGImage in coders/png.c.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5132
3980	CVE-2017-13140	MEDIUM	Medium	In ImageMagick before 6.9.9-1 and 7.x before 7.0.6-2, the ReadOnePNGImage function in coders/png.c allows remote attackers to cause a denial of service (application hang in LockSemaphoreInfo) via a PNG file with a width equal to MAGICK_WIDTH_LIMIT.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5160
3981	CVE-2017-13139	HIGH	Critical	In ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1, the ReadOneMNGImage function in coders/png.c has an out-of-bounds read with the MNG CLIP chunk.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5153
3982	CVE-2017-13134	MEDIUM	Medium	In ImageMagick 7.0.6-6, a heap-based buffer over-read was found in the function SFWScan in coders/sfw.c, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5169
3983	CVE-2017-13133	HIGH	Medium	In ImageMagick 7.0.6-8, the load_level function in coders/xcf.c lacks offset validation, which allows attackers to cause a denial of service (load_tile memory exhaustion) via a crafted file.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5131
3984	CVE-2017-13132	MEDIUM	Medium	In ImageMagick 7.0.6-8, the WritePDFImage function in coders/pdf.c operates on an incorrect data structure in the dump uncompressed PseudoColor packets step, which allows attackers to cause a denial of service (assertion failure in WriteBlobStream in MagickCore/blob.c) via a crafted file.	imagemagick	Unchanged	Not vulnerable	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5158
3985	CVE-2017-13131	MEDIUM	Medium	In ImageMagick 7.0.6-8, a memory leak vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service (memory consumption in NewLinkedList in MagickCore/linked-list.c) via a crafted file.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5142
3986	CVE-2017-13099	MEDIUM	Medium	wolfSSL prior to version 3.12.2 provides a weak Bleichenbacher oracle when any TLS cipher suite using RSA key exchange is negotiated. An attacker can recover the private key from a vulnerable wolfSSL application. This vulnerability is referred to as ROBOT.	wolfssl	Unchanged	Vulnerable	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2744
3987	CVE-2017-13090	HIGH	High	The retr.c:fd_read_body() function is called when processing OK responses. When the response is sent chunked in wget before 1.19.2, the chunk parser uses strtol() to read each chunk's length, but doesn't check that the chunk length is a non-negative number. The code then tries to read the chunk in pieces of 8192 bytes by using the MIN() macro, but ends up passing the negative chunk length to retr.c:fd_read(). As fd_read() takes an int argument, the high 32 bits of the chunk length are discarded, leaving fd_read() with a completely attacker controlled length argument. The attacker can corrupt malloc metadata after the allocated buffer.	wget	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5719
3988	CVE-2017-13089	HIGH	High	The http.c:skip_short_body() function is called in some circumstances, such as when processing redirects. When the response is sent chunked in wget before 1.19.2, the chunk parser uses strtol() to read each chunk's length, but doesn't check that the chunk length is a non-negative number. The code then tries to skip the chunk in pieces of 512 bytes by using the MIN() macro, but ends up passing the negative chunk length to connect.c:fd_read(). As fd_read() takes an int argument, the high 32 bits of the chunk length are discarded, leaving fd_read() with a completely attacker controlled length argument.	wget	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5702
3989	CVE-2017-13088	LOW	Medium	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.	wpa-supplicant & hostapd	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5522
3990	CVE-2017-13087	LOW	Medium	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.	wpa-supplicant & hostapd	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5542
3991	CVE-2017-13086	MEDIUM	Medium	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.	wpa-supplicant & hostapd	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5544
3992	CVE-2017-13084	MEDIUM	Medium	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the STK key in the PeerKey handshake.	wpa-supplicant & hostapd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5574
3993	CVE-2017-13082	MEDIUM	High	Wi-Fi Protected Access (WPA and WPA2) accepting a retransmitted Fast BSS Transition Reassociation Request and reinstalling the pairwise key while processing it.	wpa-supplicant & hostapd	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5526
3994	CVE-2017-13081	LOW	Medium	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the integrity group key in the Group Key handshake.	wpa-supplicant & hostapd	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5552
3995	CVE-2017-13080	LOW	Medium	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the group key in the Group Key handshake.	wpa-supplicant & hostapd	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5557
3996	CVE-2017-13079	LOW	Medium	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the integrity group key in the Four-way handshake.	wpa-supplicant & hostapd	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5596
3997	CVE-2017-13078	LOW	Medium	Wi-Fi Protected Access (WPA and WPA2) allowsreinstallation of the group key in the Four-way handshake.	wpa-supplicant & hostapd	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5565
3998	CVE-2017-13077	MEDIUM	Medium	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the pairwise key in the four-way handshake.	wpa-supplicant & hostapd	Unchanged	8.0.0.23	9.0.0.12	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5553
3999	CVE-2017-13062	Medium	Medium	In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function formatIPTC in coders/meta.c, which allows attackers to cause a denial of service (WriteMETAImage memory consumption) via a crafted file.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5167

	A	B	C	D	E	F	G	H	I	J	K	L	M
4000	CVE-2017-13060	Medium	Medium	In ImageMagick 7.0.6-5, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5118
4001	CVE-2017-13059	Medium	Medium	In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function WriteOneJNGImage in coders/png.c, which allows attackers to cause a denial of service (WriteJNGImage memory consumption) via a crafted file.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5164
4002	CVE-2017-13058	Medium	Medium	In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function WritePCXImage in coders/pcx.c, which allows attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5165
4003	CVE-2017-13055	HIGH	Critical	The ISO IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print_is_reach_subtlv().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5238
4004	CVE-2017-13054	HIGH	Critical	The LLDP parser in tcpdump before 4.9.2 has a buffer over-read in print-lldp.c:lldp_private_8023_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5285
4005	CVE-2017-13053	HIGH	Critical	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:decode_rt_routing_info().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5310
4006	CVE-2017-13052	HIGH	Critical	The CFM parser in tcpdump before 4.9.2 has a buffer over-read in print-cfm.c:cfm_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5224
4007	CVE-2017-13051	HIGH	Critical	The RSVP parser in tcpdump before 4.9.2 has a buffer over-read in print-rsvp.c:rsvp_obj_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5324
4008	CVE-2017-13050	HIGH	Critical	The RPKI-Router parser in tcpdump before 4.9.2 has a buffer over-read in print-rpki-rtr.c:rpki_rtr_pdu_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5315
4009	CVE-2017-13049	HIGH	Critical	The Rx protocol parser in tcpdump before 4.9.2 has a buffer over-read in print-rx.c:ubik_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5356
4010	CVE-2017-13048	HIGH	Critical	The RSVP parser in tcpdump before 4.9.2 has a buffer over-read in print-rsvp.c:rsvp_obj_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5236
4011	CVE-2017-13047	HIGH	Critical	The ISO ES-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:esis_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5323
4012	CVE-2017-13046	HIGH	Critical	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:bgp_attr_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5297
4013	CVE-2017-13045	HIGH	Critical	The VQP parser in tcpdump before 4.9.2 has a buffer over-read in print-vqp.c:vqp_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5226
4014	CVE-2017-13044	HIGH	Critical	The HNCP parser in tcpdump before 4.9.2 has a buffer over-read in print-hncp.c:dhcpv4_print().	tcpdump	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5258
4015	CVE-2017-13043	HIGH	Critical	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:decode_multicast_vpn().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5235
4016	CVE-2017-13042	HIGH	Critical	The HNCP parser in tcpdump before 4.9.2 has a buffer over-read in print-hncp.c:dhcpv6_print().	tcpdump	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5290
4017	CVE-2017-13041	HIGH	Critical	The ICMPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp6.c:icmp6_nodeinfo_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5231
4018	CVE-2017-13040	HIGH	Critical	The MPTCP parser in tcpdump before 4.9.2 has a buffer over-read in print-mptcp.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5344
4019	CVE-2017-13039	HIGH	Critical	The ISAKMP parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5398
4020	CVE-2017-13038	HIGH	Critical	The PPP parser in tcpdump before 4.9.2 has a buffer over-read in print-ppp.c:handle_mlppp().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5215
4021	CVE-2017-13037	HIGH	Critical	The IP parser in tcpdump before 4.9.2 has a buffer over-read in print-ip.c:ip_printts().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5221
4022	CVE-2017-13036	HIGH	Critical	The OSPFv3 parser in tcpdump before 4.9.2 has a buffer over-read in print-ospf6.c:ospf6_decode_v3().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5360
4023	CVE-2017-13035	HIGH	Critical	The ISO IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print_id().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5206
4024	CVE-2017-13034	HIGH	Critical	The PGM parser in tcpdump before 4.9.2 has a buffer over-read in print-pgm.c:pgm_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5287
4025	CVE-2017-13033	HIGH	Critical	The VTP parser in tcpdump before 4.9.2 has a buffer over-read in print-vtp.c:vtp_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5358
4026	CVE-2017-13032	HIGH	Critical	The RADIUS parser in tcpdump before 4.9.2 has a buffer over-read in print-radius.c:print_attr_string().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5275
4027	CVE-2017-13031	HIGH	Critical	The IPv6 fragmentation header parser in tcpdump before 4.9.2 has a buffer over-read in print-frag6.c:frag6_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5261
4028	CVE-2017-13030	HIGH	Critical	The PIM parser in tcpdump before 4.9.2 has a buffer over-read in print-pim.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5327
4029	CVE-2017-13029	HIGH	Critical	The PPP parser in tcpdump before 4.9.2 has a buffer over-read in print-ppp.c:print_ccp_config_options().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5270
4030	CVE-2017-13028	HIGH	Critical	The BOOTP parser in tcpdump before 4.9.2 has a buffer over-read in print-bootp.c:bootp_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5267
4031	CVE-2017-13027	HIGH	Critical	The LLDP parser in tcpdump before 4.9.2 has a buffer over-read in print-lldp.c:lldp_mgmt_addr_tlv_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5320
4032	CVE-2017-13026	HIGH	Critical	The ISO IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5378
4033	CVE-2017-13025	HIGH	Critical	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_opt_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5268
4034	CVE-2017-13024	HIGH	Critical	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_opt_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5211
4035	CVE-2017-13023	HIGH	Critical	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_opt_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5228
4036	CVE-2017-13022	HIGH	Critical	The IP parser in tcpdump before 4.9.2 has a buffer over-read in print-ip.c:ip_printroute().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5367
4037	CVE-2017-13021	HIGH	Critical	The ICMPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp6.c:icmp6_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5241
4038	CVE-2017-13020	HIGH	Critical	The VTP parser in tcpdump before 4.9.2 has a buffer over-read in print-vtp.c:vtp_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5316
4039	CVE-2017-13019	HIGH	Critical	The PGM parser in tcpdump before 4.9.2 has a buffer over-read in print-pgm.c:pgm_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5256
4040	CVE-2017-13018	HIGH	Critical	The PGM parser in tcpdump before 4.9.2 has a buffer over-read in print-pgm.c:pgm_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5352
4041	CVE-2017-13017	HIGH	Critical	The DHCPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-dhcp6.c:dhcp6opt_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5249
4042	CVE-2017-13016	HIGH	Critical	The ISO ES-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:esis_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5264
4043	CVE-2017-13015	HIGH	Critical	The EAP parser in tcpdump before 4.9.2 has a buffer over-read in print-eap.c:eap_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5309

	A	B	C	D	E	F	G	H	I	J	K	L	M
4044	CVE-2017-13014	HIGH	Critical	The White Board protocol parser in tcpdump before 4.9.2 has a buffer over-read in print-wb.c:wb_prep(), several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5336
4045	CVE-2017-13013	HIGH	Critical	The ARP parser in tcpdump before 4.9.2 has a buffer over-read in print-arp.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5392
4046	CVE-2017-13012	HIGH	Critical	The ICMP parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp.c:icmp_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5370
4047	CVE-2017-13011	HIGH	Critical	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer overflow in util-print.c:bittok2str_internal().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5234
4048	CVE-2017-13010	HIGH	Critical	The BEEP parser in tcpdump before 4.9.2 has a buffer over-read in print-beep.c:l_strnstart().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5318
4049	CVE-2017-13009	HIGH	Critical	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5374
4050	CVE-2017-13008	HIGH	Critical	The IEEE 802.11 parser in tcpdump before 4.9.2 has a buffer over-read in print-802_11.c:parse_elements().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5294
4051	CVE-2017-13007	HIGH	Critical	The Apple PKTAP parser in tcpdump before 4.9.2 has a buffer over-read in print-pktap.c:pktap_if_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5311
4052	CVE-2017-13006	HIGH	Critical	The L2TP parser in tcpdump before 4.9.2 has a buffer over-read in print-l2tp.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5214
4053	CVE-2017-13005	HIGH	Critical	The NFS parser in tcpdump before 4.9.2 has a buffer over-read in print-nfs.c:xid_map_enter().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5340
4054	CVE-2017-13004	HIGH	Critical	The Juniper protocols parser in tcpdump before 4.9.2 has a buffer over-read in print-juniper.c:juniper_parse_header().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5385
4055	CVE-2017-13003	HIGH	Critical	The LMP parser in tcpdump before 4.9.2 has a buffer over-read in print-lmp.c:lmp_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5295
4056	CVE-2017-13002	HIGH	Critical	The AODV parser in tcpdump before 4.9.2 has a buffer over-read in print-aodv.c:aodv_extension().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5299
4057	CVE-2017-13001	HIGH	Critical	The NFS parser in tcpdump before 4.9.2 has a buffer over-read in print-nfs.c:nfs_printfh().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5396
4058	CVE-2017-13000	HIGH	Critical	The IEEE 802.15.4 parser in tcpdump before 4.9.2 has a buffer over-read in print-802_15_4.c:ieee802_15_4_if_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5333
4059	CVE-2017-12999	HIGH	Critical	The IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5400
4060	CVE-2017-12998	HIGH	Critical	The IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print_extd_ip_reach().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5227
4061	CVE-2017-12997	MEDIUM	High	The LLDP parser in tcpdump before 4.9.2 could enter an infinite loop due to a bug in print-lldp.c:lldp_private_8021_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5373
4062	CVE-2017-12996	HIGH	Critical	The PIMv2 parser in tcpdump before 4.9.2 has a buffer over-read in print-pim.c:pimv2_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5271
4063	CVE-2017-12995	MEDIUM	High	The DNS parser in tcpdump before 4.9.2 could enter an infinite loop due to a bug in print-domain.c:ns_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5313
4064	CVE-2017-12994	HIGH	Critical	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:bgp_attr_print().	tcpdump	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5207
4065	CVE-2017-12993	HIGH	Critical	The Juniper protocols parser in tcpdump before 4.9.2 has a buffer over-read in print-juniper.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5346
4066	CVE-2017-12992	HIGH	Critical	The RIPng parser in tcpdump before 4.9.2 has a buffer over-read in print-ripng.c:ripng_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5397
4067	CVE-2017-12991	HIGH	Critical	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:bgp_attr_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5350
4068	CVE-2017-12990	MEDIUM	High	The ISAKMP parser in tcpdump before 4.9.2 could enter an infinite loop due to bugs in print-isakmp.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5326
4069	CVE-2017-12989	MEDIUM	High	The RESP parser in tcpdump before 4.9.2 could enter an infinite loop due to a bug in print-resp.c:resp_get_length().	tcpdump	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5278
4070	CVE-2017-12988	HIGH	Critical	The telnet parser in tcpdump before 4.9.2 has a buffer over-read in print-telnet.c:telnet_parse().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5369
4071	CVE-2017-12987	HIGH	Critical	The IEEE 802.11 parser in tcpdump before 4.9.2 has a buffer over-read in print-802_11.c:parse_elements().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5312
4072	CVE-2017-12986	HIGH	Critical	The IPv6 routing header parser in tcpdump before 4.9.2 has a buffer over-read in print-rt6.c:rt6_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5342
4073	CVE-2017-12985	HIGH	Critical	The IPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-ip6.c:ip6_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5390
4074	CVE-2017-12983	Medium	High	Heap-based buffer overflow in the ReadSFWImage function in coders/sfw.c in ImageMagick 7.0.6-8 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file.	imagemagick	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5139
4075	CVE-2017-12982	MEDIUM	Medium	The bmp_read_info_header function in bin/jp2/convertbmp.c in OpenJPEG 2.2.0 does not reject headers with a zero biBitCount, which allows remote attackers to cause a denial of service (memory allocation failure) in the opj_image_create function in lib/openjp2/image.c, related to the opj_aligned_alloc_n function in opj_malloc.c.	openjpeg	Unchanged	Won't Fix	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5126
4076	CVE-2017-12967	Medium	Medium	The getsym function in tekhex.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a malformed tekhex binary.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5159
4077	CVE-2017-12944	MEDIUM	High	The TIFFReadDirEntryArray function in tif_read.c in LibTIFF 4.0.8 mishandles memory allocation for short files, which allows remote attackers to cause a denial of service (allocation failure and application crash) in the TIFFFetchStripThing function in tif_dirread.c during a tiff2pdf invocation.	libtiff	Unchanged	8.0.0.28	9.0.0.18	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5134
4078	CVE-2017-12934	MEDIUM	High	ext/standard/var_unserializer.re in PHP 7.0.x before 7.0.21 and 7.1.x before 7.1.7 is prone to a heap use after free while unserializing untrusted data, related to the zval_get_type function in Zend/zend_types.h. Exploitation of this issue can have an unspecified impact on the integrity of PHP.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5146
4079	CVE-2017-12933	HIGH	Critical	The finish_nested_data function in ext/standard/var_unserializer.re in PHP before 5.6.31, 7.0.x before 7.0.21, and 7.1.x before 7.1.7 is prone to a buffer over-read while unserializing untrusted data. Exploitation of this issue can have an unspecified impact on the integrity of PHP.	php	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5129

	A	B	C	D	E	F	G	H	I	J	K	L	M
4080	CVE-2017-12932	HIGH	Critical	ext/standard/var_unserializer.re in PHP 7.0.x through 7.0.22 and 7.1.x through 7.1.8 is prone to a heap use after free while unserializing untrusted data, related to improper use of the hash API for key deletion in a situation with an invalid array size. Exploitation of this issue can have an unspecified impact on the integrity of PHP.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5136
4081	CVE-2017-12902	HIGH	Critical	The Zephyr parser in tcpdump before 4.9.2 has a buffer over-read in print-zephyr.c, several functions.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5372
4082	CVE-2017-12901	HIGH	Critical	The EIGRP parser in tcpdump before 4.9.2 has a buffer over-read in print-eigrp.c:eigrp_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5382
4083	CVE-2017-12900	HIGH	Critical	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer over-read in util-print.c:tok2strbuf().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5399
4084	CVE-2017-12899	HIGH	Critical	The DECnet parser in tcpdump before 4.9.2 has a buffer over-read in print-decnet.c:decnet_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5251
4085	CVE-2017-12898	HIGH	Critical	The NFS parser in tcpdump before 4.9.2 has a buffer over-read in print-nfs.c:interp_reply().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5339
4086	CVE-2017-12897	HIGH	Critical	The ISO CLNS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isoclns_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5334
4087	CVE-2017-12896	HIGH	Critical	The ISAKMP parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c:isakmp_rfc3948_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5376
4088	CVE-2017-12895	HIGH	Critical	The ICMP parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp.c:icmp_print().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5239
4089	CVE-2017-12894	HIGH	Critical	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer over-read in addrtoname.c:lookup_bytestring().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5242
4090	CVE-2017-12893	HIGH	Critical	The SMB/CIFS parser in tcpdump before 4.9.2 has a buffer over-read in smbutil.c:name_len().	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5218
4091	CVE-2017-12883	MEDIUM	Critical	Buffer overflow in the regular expression parser in PERL before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service (crash) or leak data from memory via vectors involving use of REXC_parse in the vFAIL macro.	perl	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5471
4092	CVE-2017-12877	Medium	Medium	Use-after-free vulnerability in the DestroyImage function in image.c in ImageMagick before 7.0.6-6 allows remote attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5308
4093	CVE-2017-12876	Medium	Medium	Heap-based buffer overflow in enhance.c in ImageMagick before 7.0.6-6 allows remote attackers to cause a denial of service via a crafted file.	imagemagick	Unchanged	Not vulnerable	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5300
4094	CVE-2017-12875	High	Medium	The WritePixelCachePixels function in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (CPU consumption) via a crafted file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5343
4095	CVE-2017-12865	High	Critical	Stack-based buffer overflow in dnsproxy.c in connman 1.34 and earlier allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted response query string passed to the name variable.	connman	Unchanged	8.0.0.30	9.0.0.21	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5319
4096	CVE-2017-12864	Medium	High	In opencv/modules/imgcodecs/src/grfmt_pxm.cpp, function ReadNumber did not checkout the input length, which lead to integer overflow. If the image is from remote, may lead to remote code execution or denial of service. This affects Opencv 3.3 and earlier.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5137
4097	CVE-2017-12863	Medium	High	In opencv/modules/imgcodecs/src/grfmt_pxm.cpp, function PxMDecoder::readData has a integer overflow when calculate src_pitch. If the image is from remote, may lead to remote code execution or denial of service. This affects Opencv 3.3 and earlier.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5150
4098	CVE-2017-12862	Medium	High	In modules/imgcodecs/src/grfmt_pxm.cpp, the length of buffer AutoBuffer _src is small than expected, which will cause copy buffer overflow later. If the image is from remote, may lead to remote code execution or denial of service. This affects Opencv 3.3 and earlier.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5141
4099	CVE-2017-12852	MEDIUM	High	The numpy.pad function in Numpy 1.13.1 and older versions is missing input validation. An empty list or ndarray will stick into an infinite loop, which can allow attackers to cause a DoS attack.	numpy	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5168
4100	CVE-2017-12847	MEDIUM	Medium	Nagios Core before 4.3.3 creates a nagios.lock PID file after dropping privileges to a non-root account, which might allow local users to kill arbitrary processes by leveraging access to this non-root account for nagios.lock modification before a root script executes a kill `cat /pathname/nagios.lock` command.	nagios-core	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5157
4101	CVE-2017-12839	Medium	HIGH	A heap-based buffer over-read in the getbits function in src/libmpg123/getbits.h in mpg123 through 1.25.5 allows remote attackers to cause a possible denial-of-service (out-of-bounds read) or possibly have unspecified other impact via a crafted mp3 file.	mpg123	Unchanged	Won't Fix	9.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4060
4102	CVE-2017-12837	MEDIUM	High	Heap-based buffer overflow in the regular expression compiler in PERL before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service (crash) via a crafted regular expression with the case-insensitive modifier.	perl	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5459
4103	CVE-2017-12814	High	Critical	Stack-based buffer overflow in the CPerlHost::Add method in win32/perlhost.h in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 on Windows allows attackers to execute arbitrary code via a long environment variable.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5520
4104	CVE-2017-12809	LOW	Medium	QEMU (aka Quick Emulator), when built with the IDE disk and CD/DVD-ROM Emulator support, allows local guest OS privileged users to cause a denial of service (NULL pointer dereference and QEMU process crash) by flushing an empty CDROM device drive.	qemu	Unchanged	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5120
4105	CVE-2017-12806	Medium	HIGH	In ImageMagick 7.0.6-6, a memory exhaustion vulnerability was found in the function format8BIM, which allows attackers to cause a denial of service.	imagemagick	Unchanged	Not vulnerable	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4058
4106	CVE-2017-12805	Medium	HIGH	In ImageMagick 7.0.6-6, a memory exhaustion vulnerability was found in the function ReadTIFFImage, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.31	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4059

	A	B	C	D	E	F	G	H	I	J	K	L	M
4107	CVE-2017-12799	MEDIUM	High	The elf_read_notesfunction in bfd/elf.c in GNU Binutils 2.29 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4978
4108	CVE-2017-12797	Medium	Medium	Integer overflow in the INT123_parse_new_id3 function in the ID3 parser in mpg123 before 1.25.5 on 32-bit platforms allows remote attackers to cause a denial of service via a crafted file, which triggers a heap-based buffer overflow.	mpg123	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5245
4109	CVE-2017-12762	HIGH	Critical	In /drivers/isdn/i4l/isdn_net.c: A user-controlled buffer is copied into a local buffer of constant size using strcpy without a length check which can cause a buffer overflow. This affects the Linux kernel 4.9-stable tree, 4.12-stable tree, 3.18-stable tree, and 4.4-stable tree.	linux	Unchanged	8.0.0.21	9.0.0.10	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5058
4110	CVE-2017-12693	High	Medium	The ReadBMPImage function in coders/bmp.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted BMP file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5381
4111	CVE-2017-12692	High	Medium	The ReadVIFFImage function in coders/viff.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted VIFF file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5307
4112	CVE-2017-12691	High	Medium	The ReadOneLayer function in coders/xcf.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.	imagemagick	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5265
4113	CVE-2017-12678	MEDIUM	High	In TagLib 1.11.1, the rebuildAggregateFrames function in id3v2framefactory.cpp has a pointer to cast vulnerability, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted audio file.	taglib	Unchanged	Not vulnerable	Not vulnerable	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-4989
4114	CVE-2017-12676	Medium	Medium	In ImageMagick 7.0.6-3, a memory leak vulnerability was found in the function ReadOneJNGImage in coders/png.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5084
4115	CVE-2017-12675	Medium	Medium	In ImageMagick 7.0.6-3, a missing check for multidimensional data was found in coders/mat.c, leading to a memory leak in the function ReadImage in MagickCore/constitute.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5061
4116	CVE-2017-12674	High	Medium	In ImageMagick 7.0.6-2, a CPU exhaustion vulnerability was found in the function ReadPDBImage in coders/pdb.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5037
4117	CVE-2017-12673	Medium	Medium	In ImageMagick 7.0.6-3, a memory leak vulnerability was found in the function ReadOneMNGImage in coders/png.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5044
4118	CVE-2017-12672	Medium	Medium	In ImageMagick 7.0.6-3, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4944
4119	CVE-2017-12671	Medium	Medium	In ImageMagick 7.0.6-3, a missing NULL assignment was found in coders/png.c, leading to an invalid free in the function RelinquishMagickMemory in MagickCore/memory.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5063
4120	CVE-2017-12670	Medium	Medium	In ImageMagick 7.0.6-3, missing validation was found in coders/mat.c, leading to an assertion failure in the function DestroyImage in MagickCore/image.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5060
4121	CVE-2017-12669	Medium	High	ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteCALSImage in coders/cals.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4969
4122	CVE-2017-12668	Medium	High	ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePCXImage in coders/pcx.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4934
4123	CVE-2017-12667	Medium	High	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadMATImage in coders\mat.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5007
4124	CVE-2017-12666	Medium	High	ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteINLINEImage in coders/inline.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5054
4125	CVE-2017-12665	Medium	High	ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePICTImage in coders/pict.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5021
4126	CVE-2017-12664	Medium	High	ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePALMImage in coders/palm.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5034
4127	CVE-2017-12663	Medium	High	ImageMagick 7.0.6-2 has a memory leak vulnerability in WriteMAPImage in coders/map.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5073
4128	CVE-2017-12662	Medium	High	ImageMagick 7.0.6-2 has a memory leak vulnerability in WritePDFImage in coders/pdf.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5066
4129	CVE-2017-12654	Medium	Medium	The ReadPICTImage function in coders/pict.c in ImageMagick 7.0.6-3 allows attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4995
4130	CVE-2017-12652	HIGH	CRITICAL	libpng before 1.6.32 does not properly check the length of chunks against the user limit.	libpng	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	Not vulnerable	10.19.45.1	Not vulnerable	LIN1018-4418
4131	CVE-2017-12644	Medium	High	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadDCMImage in coders\dcm.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5049
4132	CVE-2017-12643	High	Medium	ImageMagick 7.0.6-1 has a memory exhaustion vulnerability in ReadOneJNGImage in coders\png.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4964
4133	CVE-2017-12642	Medium	High	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadMPCImage in coders\mpc.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5067
4134	CVE-2017-12641	Medium	High	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadOneJNGImage in coders\png.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5017
4135	CVE-2017-12640	Medium	High	ImageMagick 7.0.6-1 has an out-of-bounds read vulnerability in ReadOneMNGImage in coders/png.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4948
4136	CVE-2017-12627	HIGH	CRITICAL	In Apache Xerces-C XML Parser library before 3.2.1, processing of external DTD paths can result in a null pointer dereference under certain conditions.	xerces-c	Unchanged	8.0.0.26	9.0.0.15	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3554
4137	CVE-2017-12606	Medium	High	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the function FillColorRow4 in utils.cpp when reading an image file by using cv::imread.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5002
4138	CVE-2017-12605	Medium	High	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the FillColorRow8 function in utils.cpp when reading an image file by using cv::imread.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5003

	A	B	C	D	E	F	G	H	I	J	K	L	M
4139	CVE-2017-12604	Medium	High	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the FillUniColor function in utils.cpp when reading an image file by using cv::imread.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-4962
4140	CVE-2017-12603	Medium	High	OpenCV (Open Source Computer Vision Library) through 3.3 has an invalid write in the cv::RLByteStream::getBytes function in modules/imgcodecs/src/bitstrm.cpp when reading an image file by using cv::imread, as demonstrated by the 2-opencv-heapoverflow-fseek test case.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-4973
4141	CVE-2017-12602	High	High	OpenCV (Open Source Computer Vision Library) through 3.3 has a denial of service (memory consumption) issue, as demonstrated by the 10-opencv-dos-memory-exhaust test case.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-4981
4142	CVE-2017-12601	Medium	High	OpenCV (Open Source Computer Vision Library) through 3.3 has a buffer overflow in the cv::BmpDecoder::readData function in modules/imgcodecs/src/grfmt_bmp.cpp when reading an image file by using cv::imread, as demonstrated by the 4-buf-overflow-readData-memcpy test case.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5018
4143	CVE-2017-12600	High	High	OpenCV (Open Source Computer Vision Library) through 3.3 has a denial of service (CPU consumption) issue, as demonstrated by the 11-opencv-dos-cpu-exhaust test case.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5027
4144	CVE-2017-12599	Medium	High	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds read error in the function icvCvt_BGRA2BGR_8u_C4C3R when reading an image file by using cv::imread.	opencv	Unchanged	Won't Fix	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5008
4145	CVE-2017-12598	Medium	High	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds read error in the cv::RBaseStream::readBlock function in modules/imgcodecs/src/bitstrm.cpp when reading an image file by using cv::imread, as demonstrated by the 8-opencv-invalid-read-fread test case.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5089
4146	CVE-2017-12597	Medium	High	OpenCV (Open Source Computer Vision Library) through 3.3 has an out-of-bounds write error in the function FillColorRow1 in utils.cpp when reading an image file by using cv::imread.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-5011
4147	CVE-2017-12588	HIGH	Critical	The zmq3 input and output modules in rsyslog before 8.28.0 interpreted description fields as format strings, possibly allowing a format string attack with unspecified impact.	rsyslog	Unchanged	8.0.0.21	9.0.0.10	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5074
4148	CVE-2017-12587	Medium	High	ImageMagick 7.0.6-1 has a large loop vulnerability in the ReadPWPImage function in coders\pwp.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5082
4149	CVE-2017-12566	Medium	Medium	In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadMVGImage in coders/mvg.c, which allows attackers to cause a denial of service, related to the function ReadSVGImage in svg.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4968
4150	CVE-2017-12565	Medium	Medium	In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadOneJNGImage in coders/png.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5093
4151	CVE-2017-12564	Medium	Medium	In ImageMagick 7.0.6-2, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4955
4152	CVE-2017-12563	High	Medium	In ImageMagick 7.0.6-2, a memory exhaustion vulnerability was found in the function ReadPSDImage in coders/psd.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4946
4153	CVE-2017-12459	Medium	High	The bfd_mach_o_read_symtab_strtab function in bfd/mach-o.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted mach-o file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5020
4154	CVE-2017-12458	Medium	High	The nlm_swap_auxiliary_headers_in function in bfd/nlmcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted nlm file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5075
4155	CVE-2017-12457	Medium	High	The bfd_make_section_with_flags function in section.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a NULL dereference via a crafted file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4956
4156	CVE-2017-12456	Medium	High	The read_symbol_stabs_debugging_info function in rddbg.c in GNU Binutils 2.29 and earlier allows remote attackers to cause an out of bounds heap read via a crafted binary file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4971
4157	CVE-2017-12455	Medium	High	The evax_bfd_print_emh function in vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5014
4158	CVE-2017-12454	Medium	High	The _bfd_vms_slurp_egsd function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an arbitrary memory read via a crafted vms alpha file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5064
4159	CVE-2017-12453	Medium	High	The _bfd_vms_slurp_eeom function in libbfd.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4963
4160	CVE-2017-12452	Medium	High	The bfd_mach_o_i386_canonicalize_one_relo c function in bfd/mach-o-i386.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted mach-o file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5035
4161	CVE-2017-12451	Medium	High	The _bfd_xcoff_read_ar_hdr function in bfd/coff-rs6000.c and bfd/coff64-rs6000.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds stack read via a crafted COFF image file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4974

	A	B	C	D	E	F	G	H	I	J	K	L	M
4162	CVE-2017-12450	Medium	High	The alpha_vms_object_p function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted vms alpha file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4951
4163	CVE-2017-12449	Medium	High	The _bfd_vms_save_sized_string function in vms-misc.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms file.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4925
4164	CVE-2017-12448	Medium	High	The bfd_cache_close function in bfd/cache.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a heap use after free and possibly achieve code execution via a crafted nested archive file. This issue occurs because incorrect functions are called during an attempt to release memory. The issue can be addressed by better input validation in the bfd_generic_archive_p function in bfd/archive.c.	binutils	Unchanged	8.0.0.23	9.0.0.11	10.17.41.7	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5057
4165	CVE-2017-12447	Medium	HIGH	GdkPixBuf (aka gdk-pixbuf), possibly 2.32.2, as used by GNOME Nautilus 3.14.3 on Ubuntu 16.04, allows attackers to cause a denial of service (stack corruption) or possibly have unspecified other impact via a crafted file folder.	gdk-pixbuf	Unchanged	8.0.0.30	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3754
4166	CVE-2017-12435	High	High	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadSUNImage in coders/sun.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4982
4167	CVE-2017-12434	Medium	Medium	In ImageMagick 7.0.6-1, a missing NULL check vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service (assertion failure) in DestroyImageInfo in image.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5050
4168	CVE-2017-12433	Medium	Medium	In ImageMagick 7.0.6-1, a memory leak vulnerability was found in the function ReadPESImage in coders/pes.c, which allows attackers to cause a denial of service, related to ResizeMagickMemory in memory.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5068
4169	CVE-2017-12432	High	Medium	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadPCXImage in coders/pcx.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5080
4170	CVE-2017-12431	Medium	Medium	In ImageMagick 7.0.6-1, a use-after-free vulnerability was found in the function ReadWMFImage in coders/wmf.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5053
4171	CVE-2017-12430	High	High	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMPCImage in coders/mpc.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4999
4172	CVE-2017-12429	High	High	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5055
4173	CVE-2017-12428	Medium	High	In ImageMagick 7.0.6-1, a memory leak vulnerability was found in the function ReadWMFImage in coders/wmf.c, which allows attackers to cause a denial of service in CloneDrawInfo in draw.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5085
4174	CVE-2017-12427	Medium	Medium	The ProcessMSLScript function in coders/msl.c in ImageMagick before 6.9.9-5 and 7.x before 7.0.6-5 allows remote attackers to cause a denial of service (memory leak) via a crafted file, related to the WriteMSLImage function.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5051
4175	CVE-2017-12424	HIGH	Critical	In shadow before 4.5, the newusers tool could be made to manipulate internal data structures in ways unintended by the authors. Malformed input may lead to crashes (with a buffer overflow or other memory corruption) or other unspecified behaviors. This crosses a privilege boundary in, for example, certain web-hosting environments in which a Control Panel allows an unprivileged user account to create subaccounts.	shadow	Unchanged	8.0.0.21	9.0.0.10	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4975
4176	CVE-2017-12418	Medium	High	ImageMagick 7.0.6-5 has memory leaks in the parse8BIMW and format8BIM functions in coders/meta.c, related to the WriteImage function in MagickCore/constitute.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4967
4177	CVE-2017-12380	HIGH	High	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation checking mechanisms in mbox.c during certain mail parsing functions of the ClamAV software. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted email to the affected device. An exploit could trigger a NULL pointer dereference condition when ClamAV scans the malicious email, which may result in a DoS condition.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3194
4178	CVE-2017-12379	HIGH	Critical	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or potentially execute arbitrary code on an affected device. The vulnerability is due to improper input validation checking mechanisms in the message parsing function on an affected system. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted email to the affected device. This action could cause a messageAddArgument (in message.c) buffer overflow condition when ClamAV scans the malicious email, allowing the attacker to potentially cause a DoS condition or execute arbitrary code on an affected device.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3201

	A	B	C	D	E	F	G	H	I	J	K	L	M
4179	CVE-2017-12378	HIGH	Medium	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation checking mechanisms of .tar (Tape Archive) files sent to an affected device. A successful exploit could cause a checksum buffer over-read condition when ClamAV scans the malicious .tar file, potentially allowing the attacker to cause a DoS condition on the affected device.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3205
4180	CVE-2017-12377	HIGH	Critical	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or potentially execute arbitrary code on an affected device. The vulnerability is due to improper input validation checking mechanisms in mew packet files sent to an affected device. A successful exploit could cause a heap-based buffer over-read condition in mew.c when ClamAV scans the malicious file, allowing the attacker to cause a DoS condition or potentially execute arbitrary code on the affected device.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3196
4181	CVE-2017-12376	HIGH	High	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or potentially execute arbitrary code on an affected device. The vulnerability is due to improper input validation checking mechanisms when handling Portable Document Format (.pdf) files sent to an affected device. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted .pdf file to an affected device. This action could cause a handle_pdfname (in pdf.c) buffer overflow when ClamAV scans the malicious file, allowing the attacker to cause a DoS condition or potentially execute arbitrary code.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3231
4182	CVE-2017-12375	HIGH	High	The ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a lack of input validation checking mechanisms during certain mail parsing functions (the rfc2047 function in mbox.c). An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted email to the affected device. This action could cause a buffer overflow condition when ClamAV scans the malicious email, allowing the attacker to potentially cause a DoS condition on an affected device.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3237
4183	CVE-2017-12374	HIGH	High	The ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a lack of input validation checking mechanisms during certain mail parsing operations (mbox.c operations on bounce messages). If successfully exploited, the ClamAV software could allow a variable pointing to the mail body which could cause a used after being free (use-after-free) instance which may lead to a disruption of services on an affected device to include a denial of service condition.	clamav	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3207
4184	CVE-2017-12193	MEDIUM	Medium	The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.13.11 mishandles node splitting, which allows local users to cause a denial of service (NULL pointer dereference and panic) via a crafted application, as demonstrated by the keyring key type, and key addition and link creation operations.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2621
4185	CVE-2017-12192	MEDIUM	Medium	A vulnerability was found in the Key Management sub component of the Linux kernel, where when trying to issue a KEYTCL_READ on negative key would lead to a NULL pointer dereference. A local attacker could use this flaw to crash the kernel.	linux	Unchanged	8.0.0.23	9.0.0.12	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5571
4186	CVE-2017-12190	MEDIUM	Medium	The bio_map_user_iov and bio_unmap_user functions in block/bio.c in the Linux kernel before 4.13.8 do unbalanced refcounting when a SCSI I/O vector has small consecutive buffers belonging to the same page. The bio_add_pc_page function merges them into one, but the page reference is never dropped. This causes a memory leak and possible system lockup (exploitable against the host OS by a guest OS user, if a SCSI disk is passed through to a virtual machine) due to an out-of-memory condition.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2614
4187	CVE-2017-12188	MEDIUM	High	arch/x86/kvm/mmu.c in the Linux kernel through 4.13.5, when nested virtualisation is used, does not properly traverse guest pagetable entries to resolve a guest virtual address, which allows L1 guest OS users to execute arbitrary code on the host OS or cause a denial of service (incorrect index during page walking, and host OS crash), aka an MMU potential stack buffer overrun.	linux	Unchanged	Not vulnerable	9.0.0.12	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5548
4188	CVE-2017-12187	HIGH	Critical	xorg-x11-server before 1.19.5 was missing length validation in RENDER extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3240
4189	CVE-2017-12186	HIGH	Critical	xorg-x11-server before 1.19.5 was missing length validation in X-Resource extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3176
4190	CVE-2017-12185	HIGH	Critical	xorg-x11-server before 1.19.5 was missing length validation in MIT-SCREEN-SAVER extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3200

	A	B	C	D	E	F	G	H	I	J	K	L	M
4191	CVE-2017-12184	HIGH	Critical	xorg-x11-server before 1.19.5 was missing length validation in XINERAMA extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3214
4192	CVE-2017-12183	HIGH	Critical	xorg-x11-server before 1.19.5 was missing length validation in XFIXES extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3215
4193	CVE-2017-12182	HIGH	Critical	xorg-x11-server before 1.19.5 was missing length validation in XFree86 DRI extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3241
4194	CVE-2017-12181	HIGH	Critical	xorg-x11-server before 1.19.5 was missing length validation in XFree86 DGA extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3185
4195	CVE-2017-12180	HIGH	Critical	xorg-x11-server before 1.19.5 was missing length validation in XFree86 VidModeExtension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3236
4196	CVE-2017-12179	HIGH	Critical	xorg-x11-server before 1.19.5 was vulnerable to integer overflow in (S)ProcXIBarrierReleasePointer functions allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3211
4197	CVE-2017-12178	HIGH	Critical	xorg-x11-server before 1.19.5 had wrong extra length check in ProcXIChangeHierarchy function allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3230
4198	CVE-2017-12177	HIGH	Critical	xorg-x11-server before 1.19.5 was vulnerable to integer overflow in ProcDbeGetVisualInfo function allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3174
4199	CVE-2017-12176	HIGH	Critical	xorg-x11-server before 1.19.5 was missing extra length validation in ProcEstablishConnection function allowing malicious X client to cause X server to crash or possibly execute arbitrary code.	xorg	Unchanged	8.0.0.25	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3186
4200	CVE-2017-12173	MEDIUM	HIGH	It was found that sssd's sysdb_search_user_by_upn_res() function before 1.16.0 did not sanitize requests when querying its local cache and was vulnerable to injection. In a centralized login environment, if a password hash was locally cached for a given user, an authenticated attacker could use this flaw to retrieve it.	sssd	Unchanged	Not vulnerable	Won't Fix	Won't Fix	10.18.44.15	Won't Fix	Won't Fix	LIN10-4371
4201	CVE-2017-12172	HIGH	Medium	PostgreSQL 10.x before 10.1, 9.6.x before 9.6.6, 9.5.x before 9.5.10, 9.4.x before 9.4.15, 9.3.x before 9.3.20, and 9.2.x before 9.2.24 runs under a non-root operating system account, and database superusers have effective ability to run arbitrary code under that system account. PostgreSQL provides a script for starting the database server during system boot. Packages of PostgreSQL for many operating systems provide their own, packager-authored startup implementations. Several implementations use a log file name that the database superuser can replace with a symbolic link. As root, they open(), chmod() and/or chown() this log file name. This often suffices for the database superuser to escalate to root privileges when root starts the server.	postgresql	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2608
4202	CVE-2017-12168	MEDIUM	Medium	The access_pmu_evcntr function in arch/arm64/kvm/sys_regs.c in the Linux kernel before 4.8.11 allows privileged KVM guest OS users to cause a denial of service (assertion failure and host OS crash) by accessing the Performance Monitors Cycle Count Register (PMCCNTR).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5475
4203	CVE-2017-12166	MEDIUM	High	OpenVPN versions before 2.3.3 and 2.4.x before 2.4.4 are vulnerable to a buffer overflow vulnerability when key-method 1 is used, possibly resulting in code execution.	openvpn	Unchanged	8.0.0.30	9.0.0.21	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5519
4204	CVE-2017-12164	MEDIUM	MEDIUM	A flaw was discovered in gdm 3.24.1 where gdm greeter was no longer setting the ran_once boolean during autologin. If autologin was enabled for a victim, an attacker could simply select 'login as another user' to unlock their screen.	gdm	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-7245
4205	CVE-2017-12163	MEDIUM	HIGH	All versions of Samba, client with write access to a share can cause server memory contents to be written into a file or printer. https://www.samba.org/samba/security/CVE-2017-12163.html	samba	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2480
4206	CVE-2017-12154	LOW	High	The prepare_vmcs02 function in arch/x86/kvm/vmx.c in the Linux kernel through 4.13.3 does not ensure that the CR8-load exiting and CR8-store exiting L0 vmcs02 controls exist in cases where L1 omits the use TPR shadow vmcs12 control, which allows KVM L2 guest OS users to obtain read and write access to the hardware CR8 register.	linux	Unchanged	8.0.0.23	9.0.0.11	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5428
4207	CVE-2017-12153	MEDIUM	Medium	A security flaw was discovered in the nl80211_set_rekey_data() function in net/wireless/nl80211.c in the Linux kernel through 4.13.3. This function does not check whether the required attributes are present in a Netlink request. This request can be issued by a user with the CAP_NET_ADMIN capability and may result in a NULL pointer dereference and system crash.	linux	Unchanged	8.0.0.23	9.0.0.11	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5470
4208	CVE-2017-12151	MEDIUM	HIGH	In Samba 4.1.0 to 4.6.7, a man in the middle attack can read and may alter confidential documents transferred via a client connection, which are reached via DFS redirect when the original connection used SMB3. https://www.samba.org/samba/security/CVE-2017-12151.html	samba	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2487
4209	CVE-2017-12150	MEDIUM	HIGH	A man in the middle attack may hijack client connections in Samba 3.0.25 to 4.6.7, reference https://www.samba.org/samba/security/CVE-2017-12150.html	samba	Unchanged	8.0.0.24	9.0.0.13	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2493
4210	CVE-2017-12146	MEDIUM	High	The driver_override implementation in drivers/base/platform.c in the Linux kernel before 4.12.1 allows local users to gain privileges by leveraging a race condition between a read operation and a store operation that involve different overrides.	linux	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5375

	A	B	C	D	E	F	G	H	I	J	K	L	M
4211	CVE-2017-12140	High	Medium	The ReadDCMImage function in coders\ dcm.c in ImageMagick 7.0.6-1 has an integer signedness error leading to excessive memory consumption via a crafted DCM file.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5069
4212	CVE-2017-12133	MEDIUM	Medium	The DNS stub resolver in the GNU C Library (glibc) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attackers due to IP fragmentation.	glibc	Unchanged	8.0.0.25	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5286
4213	CVE-2017-12132	Medium	Medium	The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.	glibc	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4972
4214	CVE-2017-11755	Medium	Medium	The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an AcquireSemaphoreInfo call.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4970
4215	CVE-2017-11754	Medium	Medium	The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file that is mishandled in an OpenPixelCache call.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4983
4216	CVE-2017-11753	Medium	Medium	The GetImageDepth function in MagickCore/attribute.c in ImageMagick 7.0.6-4 might allow remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted Flexible Image Transport System (FITS) file.	imagemagick	Unchanged	Not vulnerable	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4928
4217	CVE-2017-11752	Medium	Medium	The ReadMAGICKImage function in coders/magick.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4938
4218	CVE-2017-11751	Medium	Medium	The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4997
4219	CVE-2017-11750	Medium	Medium	The ReadOneJNGImage function in coders/png.c in ImageMagick 6.9.9-4 and 7.0.6-4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5000
4220	CVE-2017-11742	Medium	High	The writeRandomBytes_RtlGenRandom function in xmlparse.c in libexpat in Expat 2.2.1 and 2.2.2 on Windows allows local users to gain privileges via a Trojan horse ADVAPI32.DLL in the current working directory because of an untrusted search path, aka DLL hijacking.	expat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5028
4221	CVE-2017-11735	Medium	Medium	The vorbis_block_clear function in lib/block.c in Xiph.Org libvorbis 1.3.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ogg file.	libvorbis	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5016
4222	CVE-2017-11724	Medium	Medium	The ReadMATImage function in coders/mat.c in ImageMagick through 6.9.9-3 and 7.x through 7.0.6-3 has memory leaks involving the quantum_info and clone_info data structures.	imagemagick	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5046
4223	CVE-2017-11720	High	Critical	There is a division-by-zero vulnerability in LAME 3.99.5, caused by a malformed input file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5026
4224	CVE-2017-11719	Medium	High	The dnxhd_decode_header function in libavcodec/dnxhddec.c in FFmpeg through 3.3.2 allows remote attackers to cause a denial of service (out-of-array access) or possibly have unspecified other impact via a crafted DNxHD file.	ffmpeg	Unchanged	Won't Fix	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5087
4225	CVE-2017-11714	Medium	High	psi/ztoken.c in Artifex Ghostscript 9.21 mishandles references to the scanner state structure, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PostScript document, related to an out-of-bounds read in the igc_reloc_struct_ptr function in psi/igc.c.	ghostscript	Unchanged	8.0.0.21	9.0.0.10	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4980
4226	CVE-2017-11698	MEDIUM	High	Heap-based buffer overflow in the __get_page function in lib/dbm/src/h_page.c in Mozilla Network Security Services (NSS) allows context-dependent attackers to have unspecified impact using a crafted cert8.db file.	nss	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	10.20.9.0	LIN10-2944
4227	CVE-2017-11697	MEDIUM	High	The __hash_open function in hash.c:229 in Mozilla Network Security Services (NSS) allows context-dependent attackers to cause a denial of service (floating point exception and crash) via a crafted cert8.db file.	nss	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	10.20.9.0	LIN10-2933
4228	CVE-2017-11696	MEDIUM	High	Heap-based buffer overflow in the __hash_open function in lib/dbm/src/hash.c in Mozilla Network Security Services (NSS) allows context-dependent attackers to have unspecified impact using a crafted cert8.db file.	nss	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	10.20.9.0	LIN10-2931
4229	CVE-2017-11695	MEDIUM	High	Heap-based buffer overflow in the alloc_segs function in lib/dbm/src/hash.c in Mozilla Network Security Services (NSS) allows context-dependent attackers to have unspecified impact using a crafted cert8.db file.	nss	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	10.20.9.0	LIN10-2920
4230	CVE-2017-11684	MEDIUM	High	There is an illegal address access in the build_table function in libavcodec/bitstream.c of Libav 12.1 that will lead to remote denial of service via crafted input.	libav	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4789
4231	CVE-2017-11671	LOW	Medium	Under certain circumstances, the ix86_expand_builtin function in i386.c in GNU Compiler Collection (GCC) version 4.6, 4.7, 4.8, 4.9, 5 before 5.5, and 6 before 6.4 will generate instruction sequences that clobber the status flag of the RDRAND and RDSEED intrinsics before it can be read, potentially causing failures of these instructions to go unreported.	gcc	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4793
4232	CVE-2017-11665	Medium	High	The ff_amf_get_field_value function in libavformat/rtmppkt.c in FFmpeg 3.3.2 allows remote RTMP servers to cause a denial of service (Segmentation Violation and application crash) via a crafted stream.	ffmpeg	Unchanged	Won't Fix	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4947
4233	CVE-2017-11644	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the ReadMATImage() function in coders/mat.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4864

	A	B	C	D	E	F	G	H	I	J	K	L	M
4234	CVE-2017-11640	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to an address access exception in the WritePTIFImage() function in coders/tiff.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4806
4235	CVE-2017-11639	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WriteCIPImage() function in coders/cip.c, related to the GetPixelLuma function in MagickCore/pixel-accessor.h.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4856
4236	CVE-2017-11628	MEDIUM	High	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only relevant for PHP applications that accept untrusted input (instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.	php	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4831
4237	CVE-2017-11613	MEDIUM	Medium	In LibTIFF 4.0.8, there is a denial of service vulnerability in the TIFFOpen function. A crafted input will lead to a denial of service attack. During the TIFFOpen process, td_imagelength is not checked. The value of td_imagelength can be directly controlled by an input file. In the ChopUpSingleUncompressedStrip function, the _TIFFCheckMalloc function is called based on td_imagelength. If we set the value of td_imagelength close to the amount of system memory, it will hang the system or trigger the OOM killer.	libtiff	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4761
4238	CVE-2017-11600	MEDIUM	High	net/xfrm/xfrm_policy.c in the Linux kernel through 4.12.3, when CONFIG_XFRM_MIGRATE is enabled, does not ensure that the dir value of xfrm_userpolicy_id is XFRM_POLICY_MAX or less, which allows local users to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via an XFRM_MSG_MIGRATE xfrm Netlink message.	linux	Unchanged	8.0.0.22	9.0.0.11	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4775
4239	CVE-2017-11577	MEDIUM	High	FontForge 20161012 is vulnerable to a buffer over-read in getsid (parsettf.c) resulting in DoS or code execution via a crafted otf file.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4784
4240	CVE-2017-11576	MEDIUM	Medium	FontForge 20161012 does not ensure a positive size in a weight vector memcpy call in readcfftopdict (parsettf.c) resulting in DoS via a crafted otf file.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4758
4241	CVE-2017-11575	MEDIUM	High	FontForge 20161012 is vulnerable to a buffer over-read in strnmatch (char.c) resulting in DoS or code execution via a crafted otf file, related to a call from the readttfcopyrights function in parsettf.c.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4825
4242	CVE-2017-11574	MEDIUM	High	FontForge 20161012 is vulnerable to a heap-based buffer overflow in readcffset (parsettf.c) resulting in DoS or code execution via a crafted otf file.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4776
4243	CVE-2017-11573	MEDIUM	High	FontForge 20161012 is vulnerable to a buffer over-read in ValidatePostScriptFontName (parsettf.c) resulting in DoS or code execution via a crafted otf file.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4786
4244	CVE-2017-11572	MEDIUM	High	FontForge 20161012 is vulnerable to a heap-based buffer over-read in readcfftopdicts (parsettf.c) resulting in DoS or code execution via a crafted otf file.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4850
4245	CVE-2017-11571	MEDIUM	High	FontForge 20161012 is vulnerable to a stack-based buffer overflow in addnibble (parsettf.c) resulting in DoS or code execution via a crafted otf file.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4752
4246	CVE-2017-11570	MEDIUM	High	FontForge 20161012 is vulnerable to a buffer over-read in umodenc (parsettf.c) resulting in DoS or code execution via a crafted otf file.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4802
4247	CVE-2017-11569	MEDIUM	High	FontForge 20161012 is vulnerable to a heap-based buffer over-read in readttfcopyrights (parsettf.c) resulting in DoS or code execution via a crafted otf file.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4791
4248	CVE-2017-11568	MEDIUM	High	FontForge 20161012 is vulnerable to a heap-based buffer over-read in PSCharStringToSplines (psread.c) resulting in DoS or code execution via a crafted otf file.	fontforge	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4867
4249	CVE-2017-11552	Medium	Medium	The mad_decoder_run function in decoder.c in libmad 0.15.1b allows remote attackers to cause a denial of service (memory corruption) via a crafted MP3 file.	libmad	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4986
4250	CVE-2017-11551	Medium	Medium	The id3_field_parse function in field.c in libid3tag 0.15.1b allows remote attackers to cause a denial of service (OOM) via a crafted MP3 file.	libid3tag	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-4965
4251	CVE-2017-11550	Medium	Medium	The id3_ucs4_length function in ucs4.c in libid3tag 0.15.1b allows remote attackers to cause a denial of service (NULL Pointer Dereference and application crash) via a crafted mp3 file.	libid3tag	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-4987
4252	CVE-2017-11548	Medium	Medium	The _tokenize_matrix function in audio_out.c in Xiph.Org libao 1.2.0 allows remote attackers to cause a denial of service (memory corruption) via a crafted MP3 file.	libao	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5092
4253	CVE-2017-11545	MEDIUM	High	tcpdump 4.9.0 has a Segmentation Violation in the compressed_sl_print function in print-sl.c:253:34.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4810
4254	CVE-2017-11544	MEDIUM	High	tcpdump 4.9.0 has a Segmentation Violation in the compressed_sl_print function in print-sl.c:229:3.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4814
4255	CVE-2017-11543	HIGH	Critical	tcpdump 4.9.0 has a buffer overflow in the sliplink_print function in print-sl.c.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4841
4256	CVE-2017-11542	HIGH	Critical	tcpdump 4.9.0 has a heap-based buffer over-read in the pimv1_print function in print-pim.c.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4796
4257	CVE-2017-11541	HIGH	Critical	tcpdump 4.9.0 has a heap-based buffer over-read in the lldp_print function in print-lldp.c, related to util-print.c.	tcpdump	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4820
4258	CVE-2017-11540	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the GetPixelIndex() function, called from the WritePICONImage function in coders/xpm.c.	imagemagick	Unchanged	Not vulnerable	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4834
4259	CVE-2017-11539	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the ReadOnePNGImage() function in coders/png.c.	imagemagick	Unchanged	8.0.0.28	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4794

	A	B	C	D	E	F	G	H	I	J	K	L	M
4260	CVE-2017-11538	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteOnePNGImage() function in coders/png.c.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4764
4261	CVE-2017-11537	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Floating Point Exception (FPE) in the WritePALMImage() function in coders/palm.c, related to an incorrect bits-per-pixel calculation.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4846
4262	CVE-2017-11536	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteJP2Image() function in coders/jp2.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4824
4263	CVE-2017-11535	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WritePSImage() function in coders/ps.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4773
4264	CVE-2017-11534	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the lite_font_map() function in coders/wmf.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4751
4265	CVE-2017-11533	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WriteUILImage() function in coders/uil.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4833
4266	CVE-2017-11532	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteMPCImage() function in coders/mpc.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4805
4267	CVE-2017-11531	MEDIUM	Medium	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Memory Leak in the WriteHISTOGRAMImage() function in coders/histogram.c.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4785
4268	CVE-2017-11530	HIGH	Medium	The ReadEPTImage function in coders/ept.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4817
4269	CVE-2017-11529	MEDIUM	Medium	The ReadMATImage function in coders/mat.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4755
4270	CVE-2017-11528	MEDIUM	Medium	The ReadDIBImage function in coders/dib.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory leak) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4858
4271	CVE-2017-11527	HIGH	Medium	The ReadDPXImage function in coders/dpx.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4815
4272	CVE-2017-11526	HIGH	Medium	The ReadOneMNGImage function in coders/png.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4842
4273	CVE-2017-11525	HIGH	Medium	The ReadCINImage function in coders/cin.c in ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4777
4274	CVE-2017-11524	MEDIUM	Medium	The WriteBlob function in MagickCore/blob.c in ImageMagick before 6.9.8-10 and 7.x before 7.6.0-0 allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4763
4275	CVE-2017-11523	HIGH	Medium	The ReadTXTImage function in coders/txt.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (infinite loop) via a crafted file, because the end-of-file condition is not considered.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4807
4276	CVE-2017-11522	MEDIUM	Medium	The WriteOnePNGImage function in coders/png.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file.	imagemagick	Unchanged	Not vulnerable	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4868
4277	CVE-2017-11505	HIGH	Medium	The ReadOneJNGImage function in coders/png.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (large loop and CPU consumption) via a malformed JNG file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4821
4278	CVE-2017-11478	HIGH	Medium	The ReadOneDJVUImage function in coders/djvu.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a malformed DJVU image.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4832
4279	CVE-2017-11473	HIGH	High	Buffer overflow in the mp_override_legacy_irq() function in arch/x86/kernel/acpi/boot.c in the Linux kernel through 4.12.2 allows local users to gain privileges via a crafted ACPI table.	linux	Unchanged	8.0.0.21	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4769
4280	CVE-2017-11472	LOW	High	The acpi_ns_terminate() function in drivers/acpi/acpica/nsutils.c in the Linux kernel before 4.12 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.	linux	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4781
4281	CVE-2017-11468	MEDIUM	High	Docker Registry before 2.6.2 in Docker Distribution does not properly restrict the amount of content accepted from a user, which allows remote attackers to cause a denial of service (memory consumption) via the manifest endpoint.	docker	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4844
4282	CVE-2017-11465	HIGH	Critical	The parser_yyerror function in the UTF-8 parser in Ruby 2.4.1 allows attackers to cause a denial of service (invalid write or read) or possibly have unspecified other impact via a crafted Ruby script, related to the parser_tokadd_utf8 function in parse.y. NOTE: this might have security relevance as a bypass of a $SAFE protection mechanism.	ruby	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4771
4283	CVE-2017-11464	MEDIUM	High	A SIGFPE is raised in the function box_blur_line of rsvg-filter.c in GNOME librsvg 2.40.17 during an attempted parse of a crafted SVG file, because of incorrect protection against division by zero.	librsvg	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4863

	A	B	C	D	E	F	G	H	I	J	K	L	M
4284	CVE-2017-11462	HIGH	Critical	Double free vulnerability in MIT Kerberos 5 (aka krb5) allows attackers to have unspecified impact via vectors involving automatic deletion of security contexts on error.	krb5	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5329
4285	CVE-2017-11450	Medium	High	coders/jpeg.c in ImageMagick before 7.0.6-1 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via JPEG data that is too short.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4765
4286	CVE-2017-11449	Medium	High	coders/mpc.c in ImageMagick before 7.0.6-1 does not enable seekable streams and thus cannot validate blob sizes, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an image received from stdin.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4835
4287	CVE-2017-11448	Medium	Medium	The ReadJPEGImage function in coders/jpeg.c in ImageMagick before 7.0.6-1 allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4787
4288	CVE-2017-11447	Medium	Medium	The ReadSCREENSHOTImage function in coders/screenshot.c in ImageMagick before 7.0.6-1 has memory leaks, causing denial of service.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4801
4289	CVE-2017-11446	High	Medium	The ReadPESImage function in coders\ pes.c in ImageMagick 7.0.6-1 has an infinite loop vulnerability that can cause CPU exhaustion via a crafted PES file.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4819
4290	CVE-2017-11434	LOW	Medium	The dhcp_decode function in slirp/bootp.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (out-of-bounds read and QEMU process crash) via a crafted DHCP options string.	qemu	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4780
4291	CVE-2017-11423	MEDIUM	Medium	The cabd_read_string function in mspack/cabd.c in libmspack 0.5alpha, as used in ClamAV 0.99.2 and other products, allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a crafted CAB file.	clamav & libmspack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4778
4292	CVE-2017-11411	High	High	In Wireshark through 2.0.13 and 2.2.x through 2.2.7, the openSAFETY dissector could crash or exhaust system memory. This was addressed in epan/dissectors/packet-opensafety.c by adding length validation. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-9350.	wireshark	Unchanged	8.0.0.22	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4782
4293	CVE-2017-11410	High	High	In Wireshark through 2.0.13 and 2.2.x through 2.2.7, the WBXML dissector could go into an infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-wbxml.c by adding validation of the relationships between indexes and lengths. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-7702.	wireshark	Unchanged	Not vulnerable	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4750
4294	CVE-2017-11409	High	High	In Wireshark 2.0.0 to 2.0.13, the GPRS LLC dissector could go into a large loop. This was addressed in epan/dissectors/packet-gprs-llc.c by using a different integer data type.	wireshark	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4849
4295	CVE-2017-11408	Medium	High	In Wireshark 2.2.0 to 2.2.7 and 2.0.0 to 2.0.13, the AMQP dissector could crash. This was addressed in epan/dissectors/packet-amqp.c by checking for successful list dissection.	wireshark	Unchanged	Not vulnerable	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4818
4296	CVE-2017-11407	Medium	High	In Wireshark 2.2.0 to 2.2.7 and 2.0.0 to 2.0.13, the MQ dissector could crash. This was addressed in epan/dissectors/packet-mq.c by validating the fragment length before a reassembly attempt.	wireshark	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4840
4297	CVE-2017-11406	High	High	In Wireshark 2.2.0 to 2.2.7 and 2.0.0 to 2.0.13, the DOCSIS dissector could go into an infinite loop. This was addressed in plugins/docsis/packet-docsis.c by rejecting invalid Frame Control parameter values.	wireshark	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4774
4298	CVE-2017-11399	MEDIUM	High	Integer overflow in the ape_decode_frame function in libavcodec/apedec.c in FFmpeg through 3.3.2 allows remote attackers to cause a denial of service (out-of-array access and application crash) or possibly have unspecified other impact via a crafted APE file.	ffmpeg	Unchanged	Not vulnerable	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4798
4299	CVE-2017-11368	MEDIUM	Medium	In MIT Kerberos 5 (aka krb5) 1.7 and later, an authenticated attacker can cause a KDC assertion failure by sending invalid S4U2Self or S4U2Proxy requests.	krb5	Unchanged	8.0.0.21	9.0.0.10	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4926
4300	CVE-2017-11362	High	Critical	In PHP 7.x before 7.0.21 and 7.1.x before 7.1.7, ext/intl/msgformat/msgformat_parse.c does not restrict the locale length, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact within International Components for Unicode (ICU) for C/C++ via a long first argument to the msgfmt_parse_message function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4826
4301	CVE-2017-11360	Medium	Medium	The ReadRLEImage function in coders\ rle.c in ImageMagick 7.0.6-1 has a large loop vulnerability via a crafted rle file that triggers a huge number_pixels value.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4843
4302	CVE-2017-11352	Medium	Medium	In ImageMagick before 7.0.5-10, a crafted RLE image can trigger a crash because of incorrect EOF handling in coders/rle.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-9144.	imagemagick	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4762
4303	CVE-2017-11335	Medium	High	There is a heap based buffer overflow in tools/tiff2pdf.c of LibTIFF 4.0.8 via a PlanarConfig=Contig image, which causes a more than one hundred bytes out-of-bounds write (related to the ZIPDecode function in tif_zip.c). A crafted input may lead to a remote denial of service attack or an arbitrary code execution attack.	libtiff	Unchanged	8.0.0.21	9.0.0.9	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-4816
4304	CVE-2017-11334	Low	Medium	The address_space_write_continue function in exec.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (out-of-bounds access and guest instance crash) by leveraging use of qemu_map_ram_ptr to access guest ram block area.	qemu	Unchanged	Not vulnerable	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5013
4305	CVE-2017-11333	Medium	Medium	The vorbis_analysis_wrote function in lib/ block.c in Xiph.Org libvorbis 1.3.5 allows remote attackers to cause a denial of service (OOM) via a crafted wav file.	libvorbis	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4943

	A	B	C	D	E	F	G	H	I	J	K	L	M
4306	CVE-2017-11331	Medium	Medium	The wav_open function in oggenc/audio.c in Xiph.Org vorbis-tools 1.4.0 allows remote attackers to cause a denial of service (memory allocation error) via a crafted wav file.	vorbis-tools	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5045
4307	CVE-2017-11310	Medium	High	The read_user_chunk_callback function in coders\png.c in ImageMagick 7.0.6-1 Q16 2017-06-21 (beta) has memory leak vulnerabilities via crafted PNG files.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4855
4308	CVE-2017-11188	HIGH	High	The ReadDPXImage function in coders\dpx.c in ImageMagick 7.0.6-0 has a large loop vulnerability that can cause CPU exhaustion via a crafted DPX file, related to lack of an EOF check.	imagemagick	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4643
4309	CVE-2017-11185	MEDIUM	High	The gmp plugin in strongSwan before 5.6.0 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted RSA signature.	strongswan	Unchanged	8.0.0.26	9.0.0.15	10.17.41.6	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3577
4310	CVE-2017-11176	HIGH	Critical	The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.	linux	Unchanged	8.0.0.20	9.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4661
4311	CVE-2017-11171	MEDIUM	Medium	Bad reference counting in the context of accept_ice_connection() in gsm-xsmp-server.c in old versions of gnome-session up until version 2.29.92 allows a local attacker to establish ICE connections to gnome-session with invalid authentication data (an invalid magic cookie). Each failed authentication attempt will leak a file descriptor in gnome-session. When the maximum number of file descriptors is exhausted in the gnome-session process, it will enter an infinite loop trying to communicate without success, consuming 100% of the CPU. The graphical session associated with the gnome-session process will stop working correctly, because communication with gnome-session is no longer possible.	gnome-session	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4670
4312	CVE-2017-11170	MEDIUM	High	The ReadTGAImage function in coders\tga.c in ImageMagick 7.0.5-6 has a memory leak vulnerability that can cause memory exhaustion via invalid colors data in the header of a TGA or VST file.	imagemagick	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4652
4313	CVE-2017-11166	HIGH	Medium	The ReadXWDImage function in coders\xwd.c in ImageMagick 7.0.5-6 has a memory leak vulnerability that can cause memory exhaustion via a crafted length (number of color-map entries) field in the header of an XWD file.	imagemagick	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4667
4314	CVE-2017-11164	HIGH	High	In PCRE 8.41, the OP_KETRMAX feature in the match function in pcre_exec.c allows stack exhaustion (uncontrolled recursion) when processing a crafted regular expression.	pcre	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-4641
4315	CVE-2017-11147	MEDIUM	Critical	In PHP before 5.6.30 and 7.x before 7.0.15, the PHAR archive handler could be used by attackers supplying malicious archive files to crash the PHP interpreter or potentially disclose information due to a buffer over-read in the phar_parse_pharfile function in ext/phar/phar.c.	php	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4640
4316	CVE-2017-11146			In PHP through 5.6.31, 7.x through 7.0.21, and 7.1.x through 7.1.7, lack of bounds checks in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-11145.	php	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4646
4317	CVE-2017-11145	MEDIUM	High	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, lack of a bounds check in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to an ext/date/lib/parse_date.c out-of-bounds read affecting the php_parse_date function.	php	Unchanged	Vulnerable	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4647
4318	CVE-2017-11144	MEDIUM	High	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, the openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function, which could lead to a crash of the PHP interpreter, related to an interpretation conflict for a negative number in ext/openssl/openssl.c, and an OpenSSL documentation omission.	php	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4664
4319	CVE-2017-11143	MEDIUM	High	In PHP before 5.6.31, an invalid free in the WDDX deserialization of boolean parameters could be used by attackers able to inject XML for deserialization to crash the PHP interpreter, related to an invalid free for an empty boolean element in ext/wddx/wddx.c.	php	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4648
4320	CVE-2017-11142	HIGH	High	In PHP before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3, remote attackers could cause a CPU consumption denial of service attack by injecting long form variables, related to main/php_variables.c.	php	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4657
4321	CVE-2017-11141	HIGH	Medium	The ReadMATImage function in coders\mat.c in ImageMagick 7.0.5-6 has a memory leak vulnerability that can cause memory exhaustion via a crafted MAT file, related to incorrect ordering of a SetImageExtent call.	imagemagick	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4666
4322	CVE-2017-11126	MEDIUM	Medium	The III_i_stereo function in libmpg123/layer3.c in mpg123 through 1.25.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file that is mishandled in the code for the block_type != 2 case, a similar issue to CVE-2017-9870.	mpg123	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4674
4323	CVE-2017-11113	MEDIUM	High	In ncurses 6.0, there is a NULL Pointer Dereference in the _nc_parse_entry function of tinfo/parse_entry.c. It could lead to a remote denial of service attack if the terminfo library code is used to process untrusted terminfo data.	ncurses	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4651
4324	CVE-2017-11112	MEDIUM	High	In ncurses 6.0, there is an attempted 0xffffffffffffffff access in the append_acs function of tinfo/parse_entry.c. It could lead to a remote denial of service attack if the terminfo library code is used to process untrusted terminfo data.	ncurses	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4676

	A	B	C	D	E	F	G	H	I	J	K	L	M
4325	CVE-2017-11111	MEDIUM	High	In Netwide Assembler (NASM) 2.14rc0, preproc.c allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted file.	nasm	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-3058
4326	CVE-2017-11109	MEDIUM	High	Vim 8.0 allows attackers to cause a denial of service (invalid free) or possibly have unspecified other impact via a crafted source (aka -S) file. NOTE: there might be a limited number of scenarios in which this has security relevance.	vim	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4678
4327	CVE-2017-11108	MEDIUM	High	tcpdump 4.9.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via crafted packet data. The crash occurs in the EXTRACT_16BITS function, called from the stp_print function for the Spanning Tree Protocol.	tcpdump	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4659
4328	CVE-2017-11103	Medium	High	Heimdal before 7.4 allows remote attackers to impersonate services with Orpheus' Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unencrypted version provides an opportunity for successful server impersonation and other attacks. NOTE: this CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.	samba	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5144
4329	CVE-2017-10995	MEDIUM	Medium	The mng_get_long function in coders/png.c in ImageMagick 7.0.6-0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted MNG image.	imagemagick	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4654
4330	CVE-2017-10989	HIGH	Critical	The getNodeSize function in ext/rtree/rtree.c in SQLite through 3.19.3, as used in GDAL and other products, mishandles undersized RTree blobs in a crafted database, leading to a heap-based buffer over-read or possibly unspecified other impact.	sqlite	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4639
4331	CVE-2017-10987	Medium	High	An FR-GV-304 issue in FreeRADIUS 3.x before 3.0.15 allows DHCP - Buffer over-read in fr_dhcp_decode_suboptions() and a denial of service.	freeradius	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4808
4332	CVE-2017-10986	Medium	High	An FR-GV-303 issue in FreeRADIUS 3.x before 3.0.15 allows DHCP - Infinite read in dhcp_attr2vp() and a denial of service.	freeradius	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4788
4333	CVE-2017-10985	High	High	An FR-GV-302 issue in FreeRADIUS 3.x before 3.0.15 allows Infinite loop and memory exhaustion with 'concat' attributes and a denial of service.	freeradius	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4827
4334	CVE-2017-10984	High	Critical	An FR-GV-301 issue in FreeRADIUS 3.x before 3.0.15 allows Write overflow in data2vp_wimax() - this allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code.	freeradius	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4837
4335	CVE-2017-10983	Medium	High	An FR-GV-206 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows DHCP - Read overflow when decoding option 63 and a denial of service.	freeradius	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4797
4336	CVE-2017-10982	Medium	High	An FR-GV-205 issue in FreeRADIUS 2.x before 2.2.10 allows DHCP - Buffer over-read in fr_dhcp_decode_options() and a denial of service.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4779
4337	CVE-2017-10981	Medium	High	An FR-GV-204 issue in FreeRADIUS 2.x before 2.2.10 allows DHCP - Memory leak in fr_dhcp_decode() and a denial of service.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4865
4338	CVE-2017-10980	Medium	High	An FR-GV-203 issue in FreeRADIUS 2.x before 2.2.10 allows DHCP - Memory leak in decode_tlv() and a denial of service.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4866
4339	CVE-2017-10979	High	Critical	An FR-GV-202 issue in FreeRADIUS 2.x before 2.2.10 allows Write overflow in rad_coalesce() - this allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4804
4340	CVE-2017-10978	Medium	High	An FR-GV-201 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows Read / write overflow in make_secret() and a denial of service.	freeradius	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4853
4341	CVE-2017-10971	MEDIUM	High	In the X.Org X server before 2017-06-19, a user authenticated to an X Session could crash or execute code in the context of the X Server by exploiting a stack overflow in the endianness conversion of X Events.	xorg	Unchanged	8.0.0.20	9.0.0.9	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-4656
4342	CVE-2017-10966	HIGH	Critical	An issue was discovered in Irssi before 1.0.4. While updating the internal nick list, Irssi could incorrectly use the GHashTable interface and free the nick while updating it. This would then result in use-after-free conditions on each access of the hash table.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4653
4343	CVE-2017-10965	HIGH	Critical	An issue was discovered in Irssi before 1.0.4. When receiving messages with invalid time stamps, Irssi would try to dereference a NULL pointer.	irssi	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4650
4344	CVE-2017-10928	MEDIUM	High	In ImageMagick 7.0.6-0, a heap-based buffer over-read in the GetNextToken function in token.c allows remote attackers to obtain sensitive information from process memory or possibly have unspecified other impact via a crafted SVG document that is mishandled in the GetUserSpaceCoordinateValue function in coders/svg.c.	imagemagick	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4668
4345	CVE-2017-10911	MEDIUM	Medium	The make_response function in drivers/block/xen-blkback/blkback.c in the Linux kernel before 4.11.8 allows guest OS users to obtain sensitive information from host OS (or other guest OS) kernel memory by leveraging the copying of uninitialized padding fields in Xen block-interface response structures, aka XSA-216.	linux	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4677
4346	CVE-2017-10810	HIGH	High	Memory leak in the virtio_gpu_object_create function in drivers/gpu/drm/virtio/virtgpu_object.c in the Linux kernel through 4.11.8 allows attackers to cause a denial of service (memory consumption) by triggering object-initialization failures.	linux	Unchanged	Not vulnerable	9.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4638

	A	B	C	D	E	F	G	H	I	J	K	L	M
4347	CVE-2017-10806	Low	Medium	Stack-based buffer overflow in hw/usb/redirect.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (QEMU process crash) via vectors related to logging debug messages.	qemu	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5004
4348	CVE-2017-10790	MEDIUM	High	The _asn1_check_identifier function in GNU Libtasn1 through 4.12 causes a NULL pointer dereference and crash when reading crafted input that triggers assignment of a NULL value within an asn1_node structure. It may lead to a remote denial of service attack.	libtasn1	Unchanged	8.0.0.21	9.0.0.10	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4679
4349	CVE-2017-10784	HIGH	High	The Basic authentication code in WEBrick library in Ruby before 2.2.8, 2.3.x before 2.3.5, and 2.4.x through 2.4.1 allows remote attackers to inject terminal emulator escape sequences into its log and possibly execute arbitrary commands via a crafted user name.	ruby	Unchanged	8.0.0.23	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5454
4350	CVE-2017-10688	Medium	High	In LibTIFF 4.0.8, there is a assertion abort in the TIFFWriteDirectoryTagCheckedLong8Array function in tif_dirwrite.c. A crafted input will lead to a remote denial of service attack.	libtiff	Unchanged	8.0.0.20	9.0.0.9	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-4669
4351	CVE-2017-10685	High	Critical	In ncurses 6.0, there is a format string vulnerability in the fmt_entry function. A crafted input will lead to a remote arbitrary code execution attack.	ncurses	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4642
4352	CVE-2017-10684	High	Critical	In ncurses 6.0, there is a stack-based buffer overflow in the fmt_entry function. A crafted input will lead to a remote arbitrary code execution attack.	ncurses	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4658
4353	CVE-2017-10683	Medium	High	In mpg123 1.25.0, there is a heap-based buffer over-read in the convert_latin1 function in libmpg123/id3.c. A crafted input will lead to a remote denial of service attack.	mpg123	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4645
4354	CVE-2017-10671	Medium	High	Heap-based Buffer Overflow in the de_dotdot function in libhttpd.c in sthttpd before 2.27.1 allows remote attackers to cause a denial of service (daemon crash) or possibly have unspecified other impact via a crafted filename.	sthttpd	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4672
4355	CVE-2017-10664	Medium	High	qemu-nbd in QEMU (aka Quick Emulator) does not ignore SIGPIPE, which allows remote attackers to cause a denial of service (daemon crash) by disconnecting during a server-to-client reply attempt.	qemu	Unchanged	8.0.0.22	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4930
4356	CVE-2017-10663	High	High	The sanity_check_ckpt function in fs/f2fs/super.c in the Linux kernel before 4.12.4 does not validate the blkoff and segno arrays, which allows local users to gain privileges via unspecified vectors.	linux	Unchanged	8.0.0.22	9.0.0.11	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5117
4357	CVE-2017-10662	High	High	The sanity_check_raw_super function in fs/f2fs/super.c in the Linux kernel before 4.11.1 does not validate the segment count, which allows local users to gain privileges via unspecified vectors.	linux	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5130
4358	CVE-2017-10661	HIGH	High	Race condition in fs/timerfd.c in the Linux kernel before 4.10.15 allows local users to gain privileges or cause a denial of service (list corruption or use-after-free) via simultaneous file-descriptor operations that leverage improper might_cancel queueing.	linux	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5163
4359	CVE-2017-10388	Medium	High	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: Applies to the Java SE Kerberos client. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8134
4360	CVE-2017-10384	MEDIUM	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.57 and earlier 5.6.37 and earlier 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5716
4361	CVE-2017-10379	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	mysql	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5725
4362	CVE-2017-10378	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.11 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5684

	A	B	C	D	E	F	G	H	I	J	K	L	M
4363	CVE-2017-10365	Medium	Low	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5711
4364	CVE-2017-10357	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8106
4365	CVE-2017-10356	LOW	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, Java SE Embedded, JRockit executes to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 6.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8079
4366	CVE-2017-10355	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8085
4367	CVE-2017-10349	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8138

	A	B	C	D	E	F	G	H	I	J	K	L	M
4368	CVE-2017-10348	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8101
4369	CVE-2017-10347	MEDIUM	Medium	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8089
4370	CVE-2017-10346	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8093
4371	CVE-2017-10345	LOW	Low	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8071
4372	CVE-2017-10320	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5691

	A	B	C	D	E	F	G	H	I	J	K	L	M
4373	CVE-2017-10314	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5675
4374	CVE-2017-10313	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Group Replication GCS). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5732
4375	CVE-2017-10311	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5694
4376	CVE-2017-10296	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5695
4377	CVE-2017-10295	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.0 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8113
4378	CVE-2017-10294	Low	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5729

	A	B	C	D	E	F	G	H	I	J	K	L	M
4379	CVE-2017-10293	MEDIUM	Medium	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Javadoc). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8119
4380	CVE-2017-10286	Low	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5682
4381	CVE-2017-10285	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8125
4382	CVE-2017-10284	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Stored Procedure). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5703
4383	CVE-2017-10283	Low	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5707
4384	CVE-2017-10281	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8083

	A	B	C	D	E	F	G	H	I	J	K	L	M
4385	CVE-2017-10279	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5708
4386	CVE-2017-10277	Medium	Medium	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/Net). Supported versions that are affected are 6.9.9 and earlier. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data as well as unauthorized read access to a subset of MySQL Connectors accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5699
4387	CVE-2017-10276	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5720
4388	CVE-2017-10274	MEDIUM	Medium	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Smart Card IO). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE accessible data as well as unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N).	jdk&jre	Unchanged	8.0.0.23	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8098
4389	CVE-2017-10268	Low	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).	mysql	Unchanged	8.0.0.23	9.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5693
4390	CVE-2017-10243	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAX-WS). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5047

	A	B	C	D	E	F	G	H	I	J	K	L	M
4391	CVE-2017-10227	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5728
4392	CVE-2017-10203	Medium	Medium	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/Net). Supported versions that are affected are 6.9.9 and earlier. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5683
4393	CVE-2017-10198	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4991
4394	CVE-2017-10193	LOW	Low	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4953
4395	CVE-2017-10176	MEDIUM	High	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4996
4396	CVE-2017-10167	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5726

	A	B	C	D	E	F	G	H	I	J	K	L	M
4397	CVE-2017-10165	Medium	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5681
4398	CVE-2017-10155	Medium	High	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5722
4399	CVE-2017-10140	MEDIUM	HIGH	Postfix before 2.11.10, 3.0.x before 3.0.10, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 might allow local users to gain privileges by leveraging undocumented functionality in Berkeley DB 2.x and later, related to reading settings from DB_CONFIG in the current directory.	postfix	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3805
4400	CVE-2017-10135	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4984
4401	CVE-2017-10125	MEDIUM	High	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 7u141 and 8u131. Difficult to exploit vulnerability allows physical access to compromise Java SE. While the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: Applies to deployment of Java where the Java Auto Update is enabled. CVSS 3.0 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5033
4402	CVE-2017-10118	MEDIUM	High	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5072

	A	B	C	D	E	F	G	H	I	J	K	L	M
4403	CVE-2017-10116	MEDIUM	High	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4932
4404	CVE-2017-10115	MEDIUM	High	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5052
4405	CVE-2017-10114	MEDIUM	High	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). Supported versions that are affected are Java SE: 7u141 and 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4929
4406	CVE-2017-10111	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). The supported version that is affected is Java SE: 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5012

	A	B	C	D	E	F	G	H	I	J	K	L	M
4407	CVE-2017-10110	MEDIUM	Critical	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5001
4408	CVE-2017-10109	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4954
4409	CVE-2017-10108	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5040
4410	CVE-2017-10107	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5038

	A	B	C	D	E	F	G	H	I	J	K	L	M
4411	CVE-2017-10105	MEDIUM	Medium	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	jdk&jre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5015
4412	CVE-2017-10102	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5019
4413	CVE-2017-10101	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4945
4414	CVE-2017-10096	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5071

	A	B	C	D	E	F	G	H	I	J	K	L	M
4415	CVE-2017-10090	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5088
4416	CVE-2017-10089	MEDIUM	Critical	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: ImageIO). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5079
4417	CVE-2017-10087	MEDIUM	Critical	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5081
4418	CVE-2017-10086	MEDIUM	Critical	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JavaFX). Supported versions that are affected are Java SE: 7u141 and 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4990

	A	B	C	D	E	F	G	H	I	J	K	L	M
4419	CVE-2017-10081	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4950
4420	CVE-2017-10078	MEDIUM	High	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Scripting). The supported version that is affected is Java SE: 8u131. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE accessible data as well as unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4985
4421	CVE-2017-10074	MEDIUM	High	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4940
4422	CVE-2017-10067	MEDIUM	High	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4993
4423	CVE-2017-10053	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	jdk&jre	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5070

	A	B	C	D	E	F	G	H	I	J	K	L	M
4424	CVE-2017-1002102	MEDIUM	MEDIUM	In Kubernetes versions 1.3.x, 1.4.x, 1.5.x, 1.6.x and prior to versions 1.7.14, 1.8.9 and 1.9.4 containers using a secret, configMap, projected or downwardAPI volume can trigger deletion of arbitrary files/directories from the nodes where they are running.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3574
4425	CVE-2017-1002101	MEDIUM	CRITICAL	In Kubernetes versions 1.3.x, 1.4.x, 1.5.x, 1.6.x and prior to versions 1.7.14, 1.8.9 and 1.9.4 containers using subpath volume mounts with any volume type (including non-privileged pods, subject to file permissions) can access files/directories outside of the volume, including the host's filesystem.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3584
4426	CVE-2017-1000499	MEDIUM	High	phpMyAdmin versions 4.7.x (prior to 4.7.6.1/4.7.7) are vulnerable to a CSRF weakness. By deceiving a user to click on a crafted URL, it is possible to perform harmful database operations such as deleting records, dropping/truncating tables etc.	phpmyadmin	Unchanged	Vulnerable	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3086
4427	CVE-2017-1000494	MEDIUM	High	Uninitialized stack variable vulnerability in NameValueParserEndElt (upnpreplyparse.c) in miniupnpd < 2.0 allows an attacker to cause Denial of Service (Segmentation fault and Memory Corruption) or possibly have unspecified other impact	miniupnpd	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3099
4428	CVE-2017-1000476	HIGH	Medium	ImageMagick 7.0.7-12 Q16, a CPU exhaustion vulnerability was found in the function ReadDDSInfo in coders/dds.c, which allows attackers to cause a denial of service.	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3108
4429	CVE-2017-1000473	HIGH	High	Linux Dash up to version v2 is vulnerable to multiple command injection vulnerabilities in the way module names are parsed and then executed resulting in code execution on the server, potentially as root.	dash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-3105
4430	CVE-2017-1000472	MEDIUM	Medium	The ZipCommon::isValidPath() function in Zip/src/ZipCommon.cpp in POCO C++ Libraries before 1.8 does not properly restrict the filename value in the ZIP header, which allows attackers to conduct absolute path traversal attacks during the ZIP decompression, and possibly create or overwrite arbitrary files, via a crafted ZIP file, related to a file path injection vulnerability.	poco	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3096
4431	CVE-2017-1000460	MEDIUM	Medium	In line libavcodec/h264dec.c:500 in libav(v13_dev0), ffmpeg(n3.4), chromium(56 prior Feb 13, 2017), the return value of init_get_bits is ignored and get_ue_golomb(&gb) is called on an uninitialized get_bits context, which causes a NULL deref exception.	Libav & ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3107
4432	CVE-2017-1000456	MEDIUM	Medium	freedesktop.org libpoppler 0.60.1 fails to validate boundaries in TextPool::addWord, leading to overflow in subsequent calculations.	poppler	Unchanged	Won't Fix	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3054
4433	CVE-2017-1000450	MEDIUM	High	In opencv/modules/imgcodecs/src/utils.cpp, functions FillUniColor and FillUniGray do not check the input length, which can lead to integer overflow. If the image is from remote, may lead to remote code execution or denial of service. This affects Opencv 3.3 and earlier.	opencv	Unchanged	Won't Fix	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3063
4434	CVE-2017-1000445	MEDIUM	Medium	ImageMagick 7.0.7-1 and older version are vulnerable to null pointer dereference in the MagickCore component and might lead to denial of service	imagemagick	Unchanged	8.0.0.25	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3087
4435	CVE-2017-1000433	MEDIUM	High	pysaml2 version 4.4.0 and older accept any password when run with python optimizations enabled. This allows attackers to log in as any user without knowing their password.	python-pysaml2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3070
4436	CVE-2017-1000422	MEDIUM	High	Gnome gdk-pixbuf 2.36.8 and older is vulnerable to several integer overflow in the gif_get_lzw function resulting in memory corruption and potential code execution	gdk-pixbuf	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3053
4437	CVE-2017-1000410	MEDIUM	High	The Linux kernel version 3.3-rc1 and later is affected by a vulnerability lies in the processing of incoming L2CAP commands - ConfigRequest, and ConfigResponse messages. This info leak is a result of uninitialized stack variables that may be returned to an attacker in their uninitialized state. By manipulating the code flows that precede the handling of these configuration messages, an attacker can also gain some control over which data will be held in the uninitialized stack variables. This can allow him to bypass KASLR, and stack canaries protection - as both pointers and stack canaries may be leaked in this manner. Combining this vulnerability (for example) with the previously disclosed RCE vulnerability in L2CAP configuration parsing (CVE-2017-1000251) may allow an attacker to exploit the RCE against kernels which were built with the above mitigations. These are the specifics of this vulnerability: In the function l2cap_parse_conf_rsp and in the function l2cap_parse_conf_req the following variable is declared without initialization: struct l2cap_conf_efs efs; In addition, when parsing input configuration parameters in both of these functions, the switch case for handling EFS elements may skip the memcpy call that will write to the efs variable: ... case L2CAP_CONF_EFS: if (olen == sizeof(efs)) memcpy(&efs, (void *)val, olen); ... The olen in the above if is attacker controlled, and regardless of that if, in both of these functions the efs variable would eventually be added to the outgoing configuration request that is being built: l2cap_add_conf_opt(&ptr, L2CAP_CONF_EFS, sizeof(efs), (unsigned long) &efs); So by sending a configuration request, or response, that contains an L2CAP_CONF_EFS element, but with an element length that is not sizeof(efs) - the memcpy to the uninitialized efs variable can be avoided, and the uninitialized variable would be returned to the attacker (16 bytes).	linux	Unchanged	8.0.0.26	9.0.0.15	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2767
4438	CVE-2017-1000409	MEDIUM	High	The buffer overflow (CVE-2017-1000409) first appeared in glibc 2.5 (released on September 29, 2006) and can be triggered through the LD_LIBRARY_PATH environment variable	glibc	Unchanged	8.0.0.25	9.0.0.15	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3130

	A	B	C	D	E	F	G	H	I	J	K	L	M
4439	CVE-2017-1000408	HIGH	High	The memory leak (CVE-2017-1000408) first appeared in glibc 2.1.1 (released on May 24, 1999) and can be reached and amplified through the LD_HWCAP_MASK environment variable	glibc	Unchanged	8.0.0.25	9.0.0.15	10.17.41.9	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3129
4440	CVE-2017-1000407	MEDIUM	High	The Linux Kernel 2.6.32 and later are affected by a denial of service, by flooding the diagnostic port 0x80 an exception can be triggered leading to a kernel panic.	linux	Unchanged	8.0.0.25	9.0.0.14	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2747
4441	CVE-2017-1000405	MEDIUM	High	The Linux Kernel versions 2.6.38 through 4.14 have a problematic use of pmd_mkdirty() in the touch_pmd() function inside the THP implementation. touch_pmd() can be reached by get_user_pages(). In such case, the pmd will become dirty. This scenario breaks the new can_follow_write_pmd()'s logic - pmd can become dirty without going through a COW cycle. This bug is not as severe as the original Dirty cow because an ext4 file (or any other regular file) cannot be mapped using THP. Nevertheless, it does allow us to overwrite read-only huge pages. For example, the zero huge page and sealed shmem files can be overwritten (since their mapping can be populated using THP). Note that after the first write page-fault to the zero page, it will be replaced with a new fresh (and zeroed) thp.	linux	Unchanged	8.0.0.24	9.0.0.13	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2716
4442	CVE-2017-1000383	LOW	Medium	GNU Emacs version 25.3.1 (and other versions most likely) ignores umask when creating a backup save file ([ORIGINAL_FILENAME]~) resulting in files that may be world readable or otherwise accessible in ways not intended by the user running the emacs binary.	emacs	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-2489
4443	CVE-2017-1000382	LOW	Medium	VIM version 8.0.1187 (and other versions most likely) ignores umask when creating a swap file ([ORIGINAL_FILENAME].swp) resulting in files that may be world readable or otherwise accessible in ways not intended by the user running the vi binary.	vim	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2488
4444	CVE-2017-1000381	MEDIUM	High	The c-ares function `ares_parse_naptr_reply()`, which is used for parsing NAPTR responses, could be triggered to read memory outside of the given input buffer if the passed in DNS response packet was crafted in a particular way.	c-ares	Unchanged	Not vulnerable	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4665
4445	CVE-2017-1000380	Low	Medium	sound/core/timer.c in the Linux kernel before 4.11.5 is vulnerable to a data race in the ALSA /dev/snd/timer driver resulting in local users being able to read information belonging to other users, i.e., uninitialized memory contents may be disclosed when a read and an ioctl happen at the same time.	linux	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4488
4446	CVE-2017-1000379	HIGH	High	The Linux Kernel running on AMD64 systems will sometimes map the contents of PIE executable, the heap or ld.so to where the stack is mapped allowing attackers to more easily manipulate the stack. Linux Kernel version 4.11.5 is affected.	linux	Unchanged	8.0.0.20	9.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4512
4447	CVE-2017-1000377	MEDIUM	Medium	An issue was discovered in the size of the default stack guard page on PAX Linux (originally from GRSecurity but shipped by other Linux vendors), specifically the default stack guard page is not sufficiently large and can be jumped over (the stack guard page is bypassed), this affects PAX Linux Kernel versions as of June 19, 2017 (specific version information is not available at this time).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4563
4448	CVE-2017-1000371	HIGH	High	The offset2lib patch as used by the Linux Kernel contains a vulnerability, if RLIMIT_STACK is set to RLIM_INFINITY and 1 Gigabyte of memory is allocated (the maximum under the 1/4 restriction) then the stack will be grown down to 0x80000000, and as the PIE binary is mapped above 0x80000000 the minimum distance between the end of the PIE binary's read-write segment and the start of the stack becomes small enough that the stack guard page can be jumped over by an attacker. This affects Linux Kernel version 4.11.5. This is a different issue than CVE-2017-1000370 and CVE-2017-1000365. This issue appears to be limited to i386 based systems.	linux	Unchanged	8.0.0.19	9.0.0.8	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4518
4449	CVE-2017-1000370	HIGH	High	The offset2lib patch as used in the Linux Kernel contains a vulnerability that allows a PIE binary to be execve()'ed with 1GB of arguments or environmental strings then the stack occupies the address 0x80000000 and the PIE binary is mapped above 0x40000000 nullifying the protection of the offset2lib patch. This affects Linux Kernel version 4.11.5 and earlier. This is a different issue than CVE-2017-1000371. This issue appears to be limited to i386 based systems.	linux	Unchanged	8.0.0.19	9.0.0.8	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4553
4450	CVE-2017-1000368	HIGH	High	Todd Miller's sudo version 1.8.20p1 and earlier is vulnerable to an input validation (embedded newlines) in the get_process_ttyname() function resulting in information disclosure and command execution.	sudo	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4436
4451	CVE-2017-1000367	MEDIUM	Medium	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution.	sudo	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4425
4452	CVE-2017-1000366	HIGH	High	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.	glibc	Unchanged	8.0.0.19	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4441

	A	B	C	D	E	F	G	H	I	J	K	L	M
4453	CVE-2017-1000365	HIGH	High	The Linux Kernel imposes a size restriction on the arguments and environmental strings passed through RLIMIT_STACK/RLIM_INFINITY (1/4 of the size), but does not take the argument and environment pointers into account, which allows attackers to bypass this limitation. This affects Linux Kernel versions 4.11.5 and earlier. It appears that this feature was introduced in the Linux Kernel version 2.6.23.	linux	Unchanged	8.0.0.21	9.0.0.10	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4440
4454	CVE-2017-1000364	MEDIUM	High	An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).	linux	Unchanged	8.0.0.19	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4439
4455	CVE-2017-1000363	HIGH	High	Linux drivers/char/lp.c Out-of-Bounds Write. Due to a missing bounds check, and the fact that parport_ptr integer is static, a 'secure boot' kernel command line adversary (can happen due to bootloader vulns, e.g. Google Nexus 6's CVE-2016-10277, where due to a vulnerability the adversary has partial control over the command line) can overflow the parport_nr array in the following code, by appending many (>LP_NO) 'lp=none' arguments to the command line.	linux	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4861
4456	CVE-2017-1000257	MEDIUM	Critical	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that response says the data is zero bytes, libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function. libcurl's deliver-data function treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called on a heap based buffer that might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or just crash) and then deliver that to the application as if it was actually downloaded.	curl	Unchanged	8.0.0.24	9.0.0.13	10.17.41.3	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-2613
4457	CVE-2017-1000256	MEDIUM	High	libvirt version 2.3.0 and later is vulnerable to a bad default configuration of verify-peer=no passed to QEMU by libvirt resulting in a failure to validate SSL/TLS certificates by default.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2492
4458	CVE-2017-1000255	MEDIUM	Medium	On Linux running on PowerPC hardware (Power8 or later) a user process can craft a signal frame and then do a sigreturn so that the kernel will take an exception (interrupt), and use the r1 value *from the signal frame* as the kernel stack pointer. As part of the exception entry the content of the signal frame is written to the kernel stack, allowing an attacker to overwrite arbitrary locations with arbitrary values. The exception handling does produce an oops, and a panic if panic_on_oops=1, but only after kernel memory has been over written. This flaw was introduced in commit: 5d176f751ee3 (powerpc: tm: Enable transactional memory (TM) lazily for userspace) which was merged upstream into v4.9-rc1. Please note that kernels built with CONFIG_PPC_TRANSACTIONAL_MEM =n are not vulnerable.	linux	Unchanged	Not vulnerable	Not vulnerable	10.17.41.4	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2505
4459	CVE-2017-1000254	MEDIUM	High	libcurl may read outside of a heap allocated buffer when doing FTP. When libcurl connects to an FTP server and successfully logs in (anonymous or not), it asks the server for the current directory with the `PWD` command. The server then responds with a 257 response containing the path, inside double quotes. The returned path name is then kept by libcurl for subsequent uses. Due to a flaw in the string parser for this directory name, a directory name passed like this but without a closing double quote would lead to libcurl not adding a trailing NUL byte to the buffer holding the name. When libcurl would then later access the string, it could read beyond the allocated heap buffer and crash or wrongly access data beyond the buffer, thinking it was part of the path. A malicious server could abuse this fact and effectively prevent libcurl-based clients to work with it - the PWD command is always issued on new FTP connections and the mistake has a high chance of causing a segfault. The simple fact that this has issue remained undiscovered for this long could suggest that malformed PWD responses are rare in benign servers. We are not aware of any exploit of this flaw. This bug was introduced in commit [415d2e7cb7] (https://github.com/curl/curl/commit/415d2e7cb7), March 2005. In libcurl version 7.56.0, the parser always zero terminates the string but also rejects it if not terminated properly with a final double quote.	curl	Unchanged	8.0.0.23	9.0.0.12	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5528
4460	CVE-2017-1000253	HIGH	High	Linux distributions that have not patched their long-term kernels with https://git.kernel.org/linus/a87938b2e246b81b4fb713edb371a9fa3c5c3c86 (committed on April 14, 2015). This kernel vulnerability was fixed in April 2015 by commit a87938b2e246b81b4fb713edb371a9fa3c5c3c86 (backported to Linux 3.10.77 in May 2015), but it was not recognized as a security threat. With CONFIG_ARCH_BINFMT_ELF_RANDOMIZE_PIE enabled, and a normal top-down address allocation strategy, load_elf_binary() will attempt to map a PIE binary into an address range immediately below mm->mmap_base. Unfortunately, load_elf_binary() does not take account of the need to allocate sufficient space for the entire binary which means that, while the first PT_LOAD segment is mapped below mm->mmap_base, the subsequent PT_LOAD segment(s) end up being mapped above mm->mmap_base into the are that is supposed to be the gap between the stack and the binary.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5555

	A	B	C	D	E	F	G	H	I	J	K	L	M
4461	CVE-2017-1000252	LOW	Medium	The KVM subsystem in the Linux kernel through 4.13.3 allows guest OS users to cause a denial of service (assertion failure, and hypervisor hang or crash) via an out-of bounds guest_irq value, related to arch/x86/kvm/vmx.c and virt/kvm/eventfd.c.	linux	Unchanged	8.0.0.28	9.0.0.11	10.17.41.2	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5437
4462	CVE-2017-1000251	HIGH	High	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 3.3-rc1 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.	linux	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5314
4463	CVE-2017-1000250	LOW	Medium	All versions of the SDP server in BlueZ 5.46 and earlier are vulnerable to an information disclosure vulnerability which allows remote attackers to obtain sensitive information from the bluetoothd process memory. This vulnerability lies in the processing of SDP search attribute requests.	bluez	Unchanged	8.0.0.22	9.0.0.11	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5359
4464	CVE-2017-1000249	LOW	Medium	An issue in file() was introduced in commit 9611f31313a93aa036389c5f3b15eea53510d4d1 (Oct 2016) lets an attacker overwrite a fixed 20 bytes stack buffer with a specially crafted .notes section in an ELF binary. This was fixed in commit 35c94dc6acc418f1ad7f6241a6680e5327495793 (Aug 2017).	file	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5365
4465	CVE-2017-1000246	MEDIUM	Medium	Python package pysaml2 version 4.4.0 and earlier reuses the initialization vector across encryptions in the IDP server, resulting in weak encryption of data.	python-pysaml2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2636
4466	CVE-2017-1000159	MEDIUM	High	Command injection in evince 3.24.8 via filename when printing to PDF	evince	Unchanged	Won't Fix	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2627
4467	CVE-2017-1000158	HIGH	Critical	CPython (aka Python) up to 2.7.13 is vulnerable to an integer overflow in the PyString_DecodeEscape function in stringobject.c, resulting in heap-based buffer overflow (and possible arbitrary code execution)	python	Unchanged	8.0.0.25	9.0.0.14	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2609
4468	CVE-2017-1000122	MEDIUM	Medium	The UNIX IPC layer in WebKit, including WebKitGTK+ prior to 2.16.3, does not properly validate certain message metadata, allowing a compromised secondary process to cause a denial of service (release assertion) of the UI process. This vulnerability does not affect Apple products.	webkit	Unchanged	8.0.0.24	9.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2501
4469	CVE-2017-1000121	HIGH	Critical	The UNIX IPC layer in WebKit, including WebKitGTK+ prior to 2.16.3, does not properly validate message size metadata, allowing a compromised secondary process to trigger an integer overflow and subsequent buffer overflow in the UI process. This vulnerability does not affect Apple products.	webkit	Unchanged	8.0.0.24	9.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2509
4470	CVE-2017-1000116	HIGH	Critical	Mercurial prior to 4.3 did not adequately sanitize hostnames passed to ssh, leading to possible shell-injection attacks.	mercurial	Unchanged	8.0.0.23	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5531
4471	CVE-2017-1000115	MEDIUM	High	Mercurial prior to version 4.3 is vulnerable to a missing symlink check that can malicious repositories to modify files outside the repository	mercurial	Unchanged	8.0.0.23	9.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5595
4472	CVE-2017-1000112	MEDIUM	High	A memory corruption issue was found in the Linux kernel. When building a UFO packet with MSG_MORE __ip_append_data() calls ip_ufo_append_data() to append. However in between two send() calls, the append path can be switched from UFO to non-UFO one, which leads to a memory corruption. In case UFO packet lengths exceeds MTU, copy = maxfraglen ? skb->len Becomes negative on the non-UFO path and the branch to allocate new skb is taken. This triggers fragmentation and computation of fraggap = skb_prev->len - maxfraglen. Fraggap can exceed MTU, causing copy = datalen - transhdrlen - fraggap to become negative. Subsequently skb_copy_and_csum_bits() writes out-of-bounds.	linux	Unchanged	8.0.0.21	9.0.0.10	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5109
4473	CVE-2017-1000111	HIGH	High	A race condition issue leading to a use-after-free flaw was found in the way the raw packet sockets implementation in the Linux kernel networking subsystem handled synchronization. A local user able to open a raw packet socket (requires the CAP_NET_RAW capability) could use this flaw to elevate their privileges on the system. In a default or common use of Red Hat Enterprise Linux 6 and 7 this issue does not allow an unprivileged local user elevate their privileges on the system. In order to exploit this issue the attacker needs CAP_NET_RAW capability, which needs to be granted by the administrator to the attacker's account. Since Red Hat Enterprise Linux does not have unprivileged user namespaces enabled by default, local unprivileged users also cannot abuse namespaces to grant this capability to themselves and elevate their privileges.	linux	Unchanged	8.0.0.23	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5123
4474	CVE-2017-1000101	MEDIUM	Medium	curl supports "globbing" of URLs, in which a user can pass a numerical range to have the tool iterate over those numbers to do a sequence of transfers. In the globbing function that parses the numerical range, there was an omission that made curl read a byte beyond the end of the URL if given a carefully crafted, or just wrongly written, URL. The URL is stored in a heap based buffer, so it could then be made to wrongly read something else instead of crashing. An example of a URL that triggers the flaw would be http://ur%20[0-60000000000000000000. We are not aware of any exploit of this flaw.	curl	Unchanged	8.0.0.21	9.0.0.10	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5022

	A	B	C	D	E	F	G	H	I	J	K	L	M
4475	CVE-2017-1000100	MEDIUM	Medium	When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about 515 bytes), the file name is truncated to fit within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length. This too large value is then used in the sendto() call, making curl attempt to send more data than what is actually put into the buffer. The sendto() function will then read beyond the end of the heap based buffer. A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client hasn't restricted which protocols it allows redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protocols with --proto-redir and libcurl's with CURLOPT_REDIR_PROTOCOLS. We are not aware of any exploit of this flaw.	curl	Unchanged	8.0.0.21	9.0.0.10	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5029
4476	CVE-2017-1000099	MEDIUM	Medium	When asking to get a file from a file:// URL, libcurl provides a feature that outputs meta-data about the file using HTTP-like headers. The code doing this would send the wrong buffer to the user (stdout or the application's provide callback), which could lead to other private data from the heap to get inadvertently displayed. The wrong buffer was an uninitialized memory area allocated on the heap and if it turned out to not contain any zero byte, it would continue and display the data following that buffer in memory. We are not aware of any exploit of this flaw.	curl	Unchanged	Not vulnerable	Not vulnerable	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-5042
4477	CVE-2017-1000083	Medium	High	backend/comics/comics-document.c (aka the comic book backend) in GNOME Evince before 3.24.1 allows remote attackers to execute arbitrary commands via a .cbt file that is a TAR archive containing a filename beginning with a --command-line option substring, as demonstrated by a --checkpoint-action=exec=bash at the beginning of the filename.	evince	Unchanged	Won't Fix	9.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5220
4478	CVE-2017-1000082	HIGH	Critical	systemd v233 and earlier fails to safely parse usernames starting with a numeric digit (e.g. 0day), running the service in question with root privileges rather than the user intended.	systemd	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4673
4479	CVE-2017-1000061	MEDIUM	High	xmlsec 1.2.23 and before is vulnerable to XML External Entity Expansion when parsing crafted input documents, resulting in possible information disclosure or denial of service	xmlsec	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4857
4480	CVE-2017-1000050	Medium	High	JasPer 2.0.12 is vulnerable to a NULL pointer exception in the function jp2_encode which failed to check to see if the image contained at least one component resulting in a denial-of-service.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4756
4481	CVE-2017-1000018	Medium	High	phpMyAdmin 4.0, 4.4., and 4.6 are vulnerable to a DOS attack in the replication status by using a specially crafted table name	phpmyadmin	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4754
4482	CVE-2017-1000017	Medium	High	phpMyAdmin 4.0, 4.4 and 4.6 are vulnerable to a weakness where a user with appropriate permissions is able to connect to an arbitrary MySQL server	phpmyadmin	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4770
4483	CVE-2017-1000015	Medium	Medium	phpMyAdmin 4.0, 4.4, and 4.6 are vulnerable to a CSS injection attack through crafted cookie parameters	phpmyadmin	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4803
4484	CVE-2017-1000014	Medium	High	phpMyAdmin 4.0, 4.4, and 4.6 are vulnerable to a DOS weakness in the table editing functionality	phpmyadmin	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4811
4485	CVE-2017-1000013	Medium	Medium	phpMyAdmin 4.0, 4.4, and 4.6 are vulnerable to an open redirect weakness	phpmyadmin	Unchanged	8.0.0.21	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4828
4486	CVE-2017-0898	MEDIUM	Critical	Ruby before 2.4.2, 2.3.5, and 2.2.8 is vulnerable to a malicious format string which contains a precious specifier (*) with a huge minus value. Such situation can lead to a buffer overrun, resulting in a heap memory corruption or an information disclosure from the heap.	ruby	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5434
4487	CVE-2017-0861	MEDIUM	High	Use-after-free vulnerability in the snd_pcm_info function in the ALSA subsystem in the Linux kernel allows attackers to gain privileges via unspecified vectors.	linux	Unchanged	8.0.0.27	9.0.0.17	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4194
4488	CVE-2017-0786	MEDIUM	High	A elevation of privilege vulnerability in the Broadcom wi-fi driver. Product: Android. Versions: Android kernel. Android ID: A-37351060. References: B-V2017060101.	linux	Unchanged	8.0.0.27	9.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4226
4489	CVE-2017-0663	MEDIUM	High	libxml2: Heap-buffer-overflow in xmlAddID	libxmi2	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4385
4490	CVE-2017-0379	Medium	High	Libgcrypt before 1.8.1 does not properly consider Curve25519 side-channel attacks, which makes it easier for attackers to discover a secret key, related to cipher/ecc.c and mpi/ec.c.	libgcrypt	Unchanged	Not vulnerable	9.0.0.12	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5248
4491	CVE-2017-0357	HIGH	CRITICAL	A heap-overflow flaw exists in the -tr loader of iucode-tool starting with v1.4 and before v2.1.1, potentially leading to SIGSEGV, or heap corruption.	iucode-tool	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-3829
4492	CVE-2016-9969	Medium	HIGH	In libwebp 0.5.1, there is a double free bug in libwebpmux.	libwebp	Unchanged	Not vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4153
4493	CVE-2016-9953	HIGH	CRITICAL	curl's TLS server certificate checks are flawed on Windows CE.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3924
4494	CVE-2016-9952	MEDIUM	HIGH	curl's TLS server certificate checks are flawed on Windows CE.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3912
4495	CVE-2016-9942	HIGH	Critical	Heap-based buffer overflow in ultra.c in LibVNCClient in LibVNCServer before 0.9.11 allows remote servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted FramebufferUpdate message with the Ultra type tile, such that the LZO payload decompressed length exceeds what is specified by the tile dimensions.	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2981
4496	CVE-2016-9941	HIGH	Critical	Heap-based buffer overflow in rfbproto.c in LibVNCClient in LibVNCServer before 0.9.11 allows remote servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted FramebufferUpdate message containing a subrectangle outside of the client drawing area.	libvncserver	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2998
4497	CVE-2016-9936	HIGH	Critical	The unserialize implementation in ext/standard/var.c in PHP 7.x before 7.0.14 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted serialized data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-6834.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2994

	A	B	C	D	E	F	G	H	I	J	K	L	M
4498	CVE-2016-9935	HIGH	Critical	The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.	php	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3006
4499	CVE-2016-9934	MEDIUM	High	ext/wddx/wddx.c in PHP before 5.6.28 and 7.x before 7.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted serialized data in a wddxPacket XML document, as demonstrated by a PDORow string.	php	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3011
4500	CVE-2016-9933	MEDIUM	High	Stack consumption vulnerability in the gdImageFillToBorder function in gd.c in the GD Graphics Library (aka libgd) before 2.2.2, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (segmentation violation) via a crafted imagefilltoborder call that triggers use of a negative color value.	libgd	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2967
4501	CVE-2016-9923	LOW	Medium	Quick Emulator (Qemu) built with the 'chardev' backend support is vulnerable to a use after free issue. It could occur while hotplug and unplugging the device in the guest. A guest user/process could use this flaw to crash a Qemu process on the host resulting in DoS.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2873
4502	CVE-2016-9922	LOW	Medium	The cirrus_do_copy function in hw/display/cirrus_vga.c in QEMU (aka Quick Emulator), when cirrus graphics mode is VGA, allows local guest OS privileged users to cause a denial of service (divide-by-zero error and QEMU process crash) via vectors involving blit pitch values.	qemu	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3692
4503	CVE-2016-9921	LOW	Medium	Quick emulator (Qemu) built with the Cirrus CLGD 54xx VGA Emulator support is vulnerable to a divide by zero issue. It could occur while copying VGA data when cirrus graphics mode was set to be VGA. A privileged user inside guest could use this flaw to crash the Qemu process instance on the host, resulting in DoS.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2854
4504	CVE-2016-9919	HIGH	High	The icmp6_send function in net/ipv6/icmp.c in the Linux kernel through 4.8.12 omits a certain check of the dst data structure, which allows remote attackers to cause a denial of service (panic) via a fragmented IPv6 packet.	linux	Unchanged	Won't Fix	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2706
4505	CVE-2016-9918	MEDIUM	High	In BlueZ 5.42, an out-of-bounds read was identified in packet_hexdump function in monitor/packet.c source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2736
4506	CVE-2016-9917	MEDIUM	High	In BlueZ 5.42, a buffer overflow was observed in read_n function in tools/hcidump.c source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2701
4507	CVE-2016-9916	MEDIUM	Medium	Memory leak in hw/9pfs/9p-proxy.c in QEMU (aka Quick Emulator) allows local privileged guest OS users to cause a denial of service (host memory consumption and possibly QEMU process crash) by leveraging a missing cleanup operation in the proxy backend.	qemu	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2964
4508	CVE-2016-9915	MEDIUM	Medium	Memory leak in hw/9pfs/9p-handle.c in QEMU (aka Quick Emulator) allows local privileged guest OS users to cause a denial of service (host memory consumption and possibly QEMU process crash) by leveraging a missing cleanup operation in the handle backend.	qemu	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2970
4509	CVE-2016-9914	MEDIUM	Medium	Memory leak in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local privileged guest OS users to cause a denial of service (host memory consumption and possibly QEMU process crash) by leveraging a missing cleanup operation in FileOperations.	qemu	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3013
4510	CVE-2016-9913	MEDIUM	Medium	Memory leak in the v9fs_device_unrealize_common function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local privileged guest OS users to cause a denial of service (host memory consumption and possibly QEMU process crash) via vectors involving the order of resource cleanup.	qemu	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2968
4511	CVE-2016-9912	LOW	Medium	Quick Emulator (Qemu) built with the Virtio GPU Device emulator support is vulnerable to a memory leakage issue. It could occur while destroying gpu resource object in 'virtio_gpu_resource_destroy'. A guest user/process could use this flaw to leak host memory bytes, resulting in DoS for a host.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2858
4512	CVE-2016-9911	LOW	Medium	Quick Emulator (Qemu) built with the USB EHCI Emulation support is vulnerable to a memory leakage issue. It could occur while processing packet data in 'ehci_init_transfer'. A guest user/process could use this issue to leak host memory, resulting in DoS for a host.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2875
4513	CVE-2016-9908	LOW	Low	Quick Emulator (Qemu) built with the Virtio GPU Device emulator support is vulnerable to an information leakage issue. It could occur while processing 'VIRTIO_GPU_CMD_GET_CAPSET' command. A guest user/process could use this flaw to leak contents of the host memory bytes.	qemu	Unchanged	Not vulnerable	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2859
4514	CVE-2016-9907	LOW	Medium	Quick Emulator (Qemu) built with the USB redirector usb-guest support is vulnerable to a memory leakage flaw. It could occur while destroying the USB redirector in 'usbredir_handle_destroy'. A guest user/process could use this issue to leak host memory, resulting in DoS for a host.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2871
4515	CVE-2016-9888	MEDIUM	Medium	An error within the tar_directory_for_file() function (gsf-infile-tar.c) in GNOME Structured File Library before 1.14.41 can be exploited to trigger a Null pointer dereference and subsequently cause a crash via a crafted TAR file.	libgsf	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2754

	A	B	C	D	E	F	G	H	I	J	K	L	M
4516	CVE-2016-9866	MEDIUM	Critical	An issue was discovered in phpMyAdmin. When the arg_separator is different from its default & value, the CSRF token was not properly stripped from the return URL of the preference import action. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2731
4517	CVE-2016-9865	HIGH	Critical	An issue was discovered in phpMyAdmin. Due to a bug in serialized string parsing, it was possible to bypass the protection offered by PMA_safeUnserialize() function. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2697
4518	CVE-2016-9864	MEDIUM	High	An issue was discovered in phpMyAdmin. With a crafted username or a table name, it was possible to inject SQL statements in the tracking functionality that would run with the privileges of the control user. This gives read and write access to the tables of the configuration storage database, and if the control user has the necessary privileges, read access to some tables of the MySQL database. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2691
4519	CVE-2016-9863	MEDIUM	High	An issue was discovered in phpMyAdmin. With a very large request to table partitioning function, it is possible to invoke a Denial of Service (DoS) attack. All 4.6.x versions (prior to 4.6.5) are affected.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2756
4520	CVE-2016-9862	MEDIUM	High	An issue was discovered in phpMyAdmin. With a crafted login request it is possible to inject BBCode in the login page. All 4.6.x versions (prior to 4.6.5) are affected.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2714
4521	CVE-2016-9861	MEDIUM	High	An issue was discovered in phpMyAdmin. Due to the limitation in URL matching, it was possible to bypass the URL white-list protection. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2752
4522	CVE-2016-9860	MEDIUM	Medium	An issue was discovered in phpMyAdmin. An unauthenticated user can execute a denial of service attack when phpMyAdmin is running with $cfg['AllowArbitraryServer']=true. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2683
4523	CVE-2016-9859	MEDIUM	Medium	An issue was discovered in phpMyAdmin. With a crafted request parameter value it is possible to initiate a denial of service attack in import feature. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2741
4524	CVE-2016-9858	MEDIUM	Medium	An issue was discovered in phpMyAdmin. With a crafted request parameter value it is possible to initiate a denial of service attack in saved searches feature. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2746
4525	CVE-2016-9857	MEDIUM	Medium	An issue was discovered in phpMyAdmin. XSS is possible because of a weakness in a regular expression used in some JavaScript processing. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2738
4526	CVE-2016-9856	MEDIUM	Medium	An XSS issue was discovered in phpMyAdmin because of an improper fix for CVE-2016-2559 in PMASA-2016-10. This issue is resolved by using a copy of a hash to avoid a race condition. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2726
4527	CVE-2016-9855	MEDIUM	Medium	An issue was discovered in phpMyAdmin. By calling some scripts that are part of phpMyAdmin in an unexpected way, it is possible to trigger phpMyAdmin to display a PHP error message which contains the full path of the directory where phpMyAdmin is installed. During an execution timeout in the export functionality, the errors containing the full path of the directory of phpMyAdmin are written to the export file. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected. This CVE is for the PMA_shutdownDuringExport issue.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2717
4528	CVE-2016-9854	MEDIUM	Medium	An issue was discovered in phpMyAdmin. By calling some scripts that are part of phpMyAdmin in an unexpected way, it is possible to trigger phpMyAdmin to display a PHP error message which contains the full path of the directory where phpMyAdmin is installed. During an execution timeout in the export functionality, the errors containing the full path of the directory of phpMyAdmin are written to the export file. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected. This CVE is for the json_decode issue.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2671
4529	CVE-2016-9853	MEDIUM	Medium	An issue was discovered in phpMyAdmin. By calling some scripts that are part of phpMyAdmin in an unexpected way, it is possible to trigger phpMyAdmin to display a PHP error message which contains the full path of the directory where phpMyAdmin is installed. During an execution timeout in the export functionality, the errors containing the full path of the directory of phpMyAdmin are written to the export file. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected. This CVE is for the fopen wrapper issue.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2703

	A	B	C	D	E	F	G	H	I	J	K	L	M
4530	CVE-2016-9852	MEDIUM	Medium	An issue was discovered in phpMyAdmin. By calling some scripts that are part of phpMyAdmin in an unexpected way, it is possible to trigger phpMyAdmin to display a PHP error message which contains the full path of the directory where phpMyAdmin is installed. During an execution timeout in the export functionality, the errors containing the full path of the directory of phpMyAdmin are written to the export file. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected. This CVE is for the curl wrapper issue.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2773
4531	CVE-2016-9851	MEDIUM	Medium	An issue was discovered in phpMyAdmin. With a crafted request parameter value it is possible to bypass the logout timeout. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2782
4532	CVE-2016-9850	MEDIUM	Medium	An issue was discovered in phpMyAdmin. Username matching for the allow/deny rules may result in wrong matches and detection of the username in the rule due to non-constant execution time. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2718
4533	CVE-2016-9849	HIGH	Critical	An issue was discovered in phpMyAdmin. It is possible to bypass AllowRoot restriction ($cfg['Servers'][$i]['AllowRoot']) and deny rules for username by using Null Byte in the username. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2767
4534	CVE-2016-9848	MEDIUM	Medium	An issue was discovered in phpMyAdmin. phpinfo (phpinfo.php) shows PHP information including values of HttpOnly cookies. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2666
4535	CVE-2016-9847	MEDIUM	Medium	An issue was discovered in phpMyAdmin. When the user does not specify a blowfish_secret key for encrypting cookies, phpMyAdmin generates one at runtime. A vulnerability was reported where the way this value is created uses a weak algorithm. This could allow an attacker to determine the user's blowfish_secret and potentially decrypt their cookies. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2778
4536	CVE-2016-9846	MEDIUM	Medium	QEMU (aka Quick Emulator) built with the Virtio GPU Device emulator support is vulnerable to a memory leakage issue. It could occur while updating the cursor data in update_cursor_data_virgl. A guest user/process could use this flaw to leak host memory bytes, resulting in DoS for a host.	qemu	Unchanged	Not vulnerable	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2974
4537	CVE-2016-9845	LOW	Medium	QEMU (aka Quick Emulator) built with the Virtio GPU Device emulator support is vulnerable to an information leakage issue. It could occur while processing 'VIRTIO_GPU_CMD_GET_CAPSET_INFO' command. A guest user/process could use this flaw to leak contents of the host memory bytes.	qemu	Unchanged	Not vulnerable	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2982
4538	CVE-2016-9844	LOW	Medium	Buffer overflow in the zi_short function in zipinfo.c in Info-Zip UnZip 6.0 allows remote attackers to cause a denial of service (crash) via a large compression method value in the central directory file header.	unzip	Unchanged	8.0.0.15	9.0.0.4	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-3232
4539	CVE-2016-9843	HIGH	Critical	zlib: Big-endian out-of-bounds pointer	zlib	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3953
4540	CVE-2016-9842	MEDIUM	High	zlib: Undefined left shift of negative number	zlib	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3897
4541	CVE-2016-9841	HIGH	Critical	inftrees.c was subtracting an offset from a pointer to an array, in order to provide a pointer that allowed indexing starting at the offset. This is not compliant with the C standard, for which the behavior of a pointer decremented before its allocated memory is undefined.	zlib	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3938
4542	CVE-2016-9840	MEDIUM	High	zlib: Out-of-bounds pointer arithmetic in inftrees.c	zlib	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3889
4543	CVE-2016-9826	MEDIUM	Medium	libavcodec/tuh263dec.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	libav	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3576
4544	CVE-2016-9825	MEDIUM	Medium	libswscale/utils.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	libav	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3565
4545	CVE-2016-9824	MEDIUM	Medium	Integer overflow in libswscale/x86/swscale.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via a crafted file.	libav	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3564
4546	CVE-2016-9823	MEDIUM	Medium	libavcodec/x86/mpegvideo.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via a crafted file.	libav	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-3577
4547	CVE-2016-9822	MEDIUM	Medium	Integer overflow in libavcodec/mpeg12dec.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via a crafted file.	libav	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3555
4548	CVE-2016-9821	MEDIUM	Medium	Integer overflow in libavcodec/mpegvideo_parser.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via a crafted file.	libav	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3572
4549	CVE-2016-9819	MEDIUM	Medium	libavcodec/mpegvideo.c in libav 11.8 allows remote attackers to cause a denial of service (crash) via vectors involving left shift of a negative value.	libav	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3518
4550	CVE-2016-9813	MEDIUM	Medium	The _parse_pat function in the mpegts parser in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted file.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3090
4551	CVE-2016-9812	MEDIUM	High	The gst_mpegts_section_new function in the mpegts decoder in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a too small section.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3078
4552	CVE-2016-9811	MEDIUM	Medium	The windows_icon_typefind function in gst-plugins-base in GStreamer before 1.10.2, when G_SLICE is set to always-malloc, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted ico file.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3087

	A	B	C	D	E	F	G	H	I	J	K	L	M
4553	CVE-2016-9810	MEDIUM	Medium	The gst_decode_chain_free_internal function in the flxdex decoder in gst-plugins-good in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (invalid memory read and crash) via an invalid file, which triggers an incorrect unref call.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3085
4554	CVE-2016-9809	MEDIUM	High	Off-by-one error in the gst_h264_parse_set_caps function in GStreamer before 1.10.2 allows remote attackers to have unspecified impact via a crafted file, which triggers an out-of-bounds read.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3081
4555	CVE-2016-9808	MEDIUM	High	The FLIC decoder in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (out-of-bounds write and crash) via a crafted series of skip and count pairs.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3082
4556	CVE-2016-9807	MEDIUM	Medium	The flx_decode_chunks function in gst/flx/gstflxdec.c in GStreamer before 1.10.2 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted FLIC file.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3086
4557	CVE-2016-9806	HIGH	High	Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows local users to cause a denial of service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg system calls, leading to a free operation associated with a new dump that started earlier than anticipated.	linux	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2862
4558	CVE-2016-9804	MEDIUM	Medium	In BlueZ 5.42, a buffer overflow was observed in commands_dump function in tools/parser/csr.c source file. The issue exists because commands array is overflowed by supplied parameter due to lack of boundary checks on size of the buffer from frame frm->ptr parameter. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2716
4559	CVE-2016-9803	MEDIUM	Medium	In BlueZ 5.42, an out-of-bounds read was observed in le_meta_ev_dump function in tools/parser/hci.c source file. This issue exists because 'subevent' (which is used to read correct element from 'ev_le_meta_str' array) is overflowed.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2705
4560	CVE-2016-9802	MEDIUM	Medium	In BlueZ 5.42, a buffer over-read was identified in l2cap_packet function in monitor/packet.c source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2674
4561	CVE-2016-9801	MEDIUM	Medium	In BlueZ 5.42, a buffer overflow was observed in set_ext_ctrl function in tools/parser/l2cap.c source file when processing corrupted dump file.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2692
4562	CVE-2016-9800	MEDIUM	Medium	In BlueZ 5.42, a buffer overflow was observed in pin_code_reply_dump function in tools/parser/hci.c source file. The issue exists because pin array is overflowed by supplied parameter due to lack of boundary checks on size of the buffer from frame pin_code_reply_cp *cp parameter.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2760
4563	CVE-2016-9799	MEDIUM	Medium	In BlueZ 5.42, a buffer overflow was observed in pklg_read_hci function in btsnoop.c source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2663
4564	CVE-2016-9798	MEDIUM	Medium	In BlueZ 5.42, a use-after-free was identified in conf_opt function in tools/parser/l2cap.c source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2668
4565	CVE-2016-9797	MEDIUM	Medium	In BlueZ 5.42, a buffer over-read was observed in l2cap_dump function in tools/parser/l2cap.c source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash.	bluez	Unchanged	8.0.0.28	9.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2681
4566	CVE-2016-9794	HIGH	High	Race condition in the snd_pcm_period_elapsed function in sound/core/pcm_lib.c in the ALSA subsystem in the Linux kernel before 4.7 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted SNDRV_PCM_TRIGGER_START command.	linux	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2876
4567	CVE-2016-9793	HIGH	High	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFFORCE or (2) SO_RCVBUFFORCE option.	linux	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2855
4568	CVE-2016-9778	MEDIUM	MEDIUM	An error handling certain queries using the nxdomain-redirect feature could cause a REQUIRE assertion failure in db.c	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2973
4569	CVE-2016-9777	MEDIUM	High	KVM in the Linux kernel before 4.8.12, when I/O APIC is enabled, does not properly restrict the VCPU index, which allows guest OS users to gain host OS privileges or cause a denial of service (out-of-bounds array access and host OS crash) via a crafted interrupt request, related to arch/x86/kvm/ioapic.c and arch/x86/kvm/ioapic.h.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2874
4570	CVE-2016-9776	LOW	Medium	QEMU (aka Quick Emulator) built with the ColdFire Fast Ethernet Controller emulator support is vulnerable to an infinite loop issue. It could occur while receiving packets in 'mcf_fec_receive'. A privileged user/process inside guest could use this issue to crash the QEMU process on the host leading to DoS.	qemu	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2997
4571	CVE-2016-9773	MEDIUM	Medium	Heap-based buffer overflow in the IsPixelGray function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.8 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted image file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9556.	imagemagick	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3401
4572	CVE-2016-9756	LOW	Medium	arch/x86/kvm/emulate.c in the Linux kernel before 4.8.12 does not properly initialize Code Segment (CS) in certain error cases, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2857

	A	B	C	D	E	F	G	H	I	J	K	L	M
4573	CVE-2016-9755	MEDIUM	High	The netfilter subsystem in the Linux kernel before 4.9 mishandles IPv6 reassembly, which allows local users to cause a denial of service (integer overflow, out-of-bounds write, and GPF) or possibly have unspecified other impact via a crafted application that makes socket, connect, and writev system calls, related to net/ipv6/netfilter/nf_conntrack_reasm.c and net/ipv6/netfilter/nf_defrag_ipv6_hooks.c.	linux	Unchanged	Not vulnerable	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2870
4574	CVE-2016-9754	HIGH	High	The ring_buffer_resize function in kernel/trace/ring_buffer.c in the profiling subsystem in the Linux kernel before 4.6.1 mishandles certain integer calculations, which allows local users to gain privileges by writing to the /sys/kernel/debug/tracing/buffer_size_kb file.	linux	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2978
4575	CVE-2016-9685	MEDIUM	Medium	Multiple memory leaks in error paths in fs/xfs/xfs_attr_list.c in the Linux kernel before 4.5.1 allow local users to cause a denial of service (memory consumption) via crafted XFS filesystem operations.	linux	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2877
4576	CVE-2016-9675	MEDIUM	High	openjpeg: A heap-based buffer overflow flaw was found in the patch for CVE-2013-6045. A crafted j2k image could cause the application to crash, or potentially execute arbitrary code.	openjpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2881
4577	CVE-2016-9644	HIGH	High	The __get_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel 4.4.22 through 4.4.28 contains extended asm statements that are incompatible with the exception table, which allows local users to obtain root access on non-SMEP platforms via a crafted application. NOTE: this vulnerability exists because of incorrect backporting of the CVE-2016-9178 patch to older kernels.	linux	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2737
4578	CVE-2016-9643	MEDIUM	High	The regex code in Webkit 2.4.11 allows remote attackers to cause a denial of service (memory consumption) as demonstrated in a large number of ($ (open parenthesis and dollar) followed by {-2,16} and a large number of +) (plus close parenthesis).	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3554
4579	CVE-2016-9642	MEDIUM	Medium	JavaScriptCore in WebKit allows attackers to cause a denial of service (out-of-bounds heap read) via a crafted Javascript file.	webkit	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-3298
4580	CVE-2016-9636	HIGH	Critical	Heap-based buffer overflow in the flx_decode_delta_fli function in gst/flx/gstflxdec.c in the FLIC decoder in GStreamer before 1.10.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by providing a 'write count' that goes beyond the initialized buffer.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3104
4581	CVE-2016-9635	HIGH	Critical	Heap-based buffer overflow in the flx_decode_delta_fli function in gst/flx/gstflxdec.c in the FLIC decoder in GStreamer before 1.10.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by providing a 'skip count' that goes beyond initialized buffer.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3103
4582	CVE-2016-9634	HIGH	Critical	Heap-based buffer overflow in the flx_decode_delta_fli function in gst/flx/gstflxdec.c in the FLIC decoder in GStreamer before 1.10.2 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via the start_line parameter.	gstreamer	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3102
4583	CVE-2016-9604	LOW	MEDIUM	It was found that it is possible for root to gain direct access to an internal keyring, such as '.builtin_trusted_keys' upstream, by joining it as its session keyring. This allows root to bypass module signature verification by adding a new public key of its own devising to the keyring.	linux	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4184
4584	CVE-2016-9603	HIGH	CRITICAL	Quick Emulator(Qemu) built with the Cirrus CLGD 54xx VGA Emulator and the VNC display driver support is vulnerable to a heap buffer overflow issue. It could occur when Vnc client attempts to update its display after a vga operation is performed by a guest.	qemu	Unchanged	8.0.0.27	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4187
4585	CVE-2016-9602	HIGH	HIGH	Qemu before version 2.9 is vulnerable to an improper link following when built with the VirtFS. A privileged user inside guest could use this flaw to access host file system beyond the shared folder and potentially escalating their privileges on a host.	qemu	Unchanged	8.0.0.28	9.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3843
4586	CVE-2016-9601	MEDIUM	MEDIUM	ghostscript before version 0.14 is vulnerable to a heap based buffer overflow that was found in the ghostscript jbig2_decode_gray_scale_image function which is used to decode halftone segments in a JBIG2 image. A document (PostScript or PDF) with an embedded, specially crafted, jbig2 image could trigger a segmentation fault in ghostscript.	ghostscript	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3812
4587	CVE-2016-9600	MEDIUM	MEDIUM	JasPer before version 2.0.10 is vulnerable to a null pointer dereference was found in the decoded creation of JPEG 2000 image files. A specially crafted file could cause an application using JasPer to crash.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3517
4588	CVE-2016-9594	MEDIUM	HIGH	libcurl's (new) internal function that returns a good 32bit random value was implemented poorly and overwrote the pointer instead of writing the value into the buffer the pointer pointed to.	libcurl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2903
4589	CVE-2016-9591	MEDIUM	MEDIUM	JasPer before version 2.0.12 is vulnerable to a use-after-free in the way it decodes certain JPEG 2000 image files resulting in a crash on the application using JasPer.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3573
4590	CVE-2016-9588	LOW	Medium	arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows guest OS users to cause a denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest.	linux	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2865
4591	CVE-2016-9586	MEDIUM	HIGH	libcurl's implementation of the printf() functions triggers a buffer overflow when doing a large floating point output. The bug occurs when the conversion outputs more than 255 bytes.	libcurl	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2902
4592	CVE-2016-9584	MEDIUM	Critical	libical allows remote attackers to cause a denial of service (use-after-free) and possibly read heap memory via a crafted ics file.	libical	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3175

	A	B	C	D	E	F	G	H	I	J	K	L	M
4593	CVE-2016-9583	MEDIUM	HIGH	An out-of-bounds heap read vulnerability was found in the jpc_pi_nextpcrl() function of jasper before 2.0.6 when processing crafted input.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4529
4594	CVE-2016-9581	MEDIUM	HIGH	An infinite loop vulnerability in tiftoimage that results in heap buffer overflow in convert_32s_C1P1 was found in openjpeg 2.1.2.	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4531
4595	CVE-2016-9580	MEDIUM	HIGH	An integer overflow vulnerability was found in tiftoimage function in openjpeg 2.1.2, resulting in heap buffer overflow.	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4528
4596	CVE-2016-9579	MEDIUM	HIGH	A flaw was found in the way Ceph Object Gateway would process cross-origin HTTP requests if the CORS policy was set to allow origin on a bucket. A remote unauthenticated attacker could use this flaw to cause denial of service by sending a specially-crafted cross-origin HTTP request. Ceph branches 1.3.x and 2.x are affected.	ceph	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4522
4597	CVE-2016-9578	MEDIUM	HIGH	A vulnerability was discovered in SPICE before 0.13.90 in the server's protocol handling. An attacker able to connect to the SPICE server could send crafted messages which would cause the process to crash.	spice	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4422
4598	CVE-2016-9577	MEDIUM	HIGH	A vulnerability was discovered in SPICE before 0.13.90 in the server's protocol handling. An authenticated attacker could send crafted messages to the SPICE server causing a heap overflow leading to a crash or possible code execution.	spice	Unchanged	8.0.0.27	9.0.0.18	10.17.41.10	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4417
4599	CVE-2016-9576	HIGH	High	The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 4.8.14 does not properly restrict the type of iterator, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device.	linux	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2869
4600	CVE-2016-9574	MEDIUM	MEDIUM	nss before version 3.30 is vulnerable to a remote denial of service during the session handshake when using SessionTicket extension and ECDHE-ECDSA.	nss	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4458
4601	CVE-2016-9573	MEDIUM	HIGH	An out-of-bounds read vulnerability was found in OpenJPEG 2.1.2, in the j2k_to_image tool. Converting a specially crafted JPEG2000 file to another format could cause the application to crash or, potentially, disclose some data from the heap.	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4550
4602	CVE-2016-9572	MEDIUM	MEDIUM	A NULL pointer dereference flaw was found in the way openjpeg 2.1.2 decoded certain input images. Due to a logic error in the code responsible for decoding the input image, an application using openjpeg to process image data could crash when processing a crafted image.	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4552
4603	CVE-2016-9561	MEDIUM	Medium	The che_configure function in libavcodec/aacdec_template.c in FFmpeg before 3.2.1 allows remote attackers to cause a denial of service (allocation of huge memory, and being killed by the OS) via a crafted MOV file.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2860
4604	CVE-2016-9560	MEDIUM	High	Stack-based buffer overflow in the jpc_tsfb_getbands2 function in jpc_tsfb.c in JasPer before 1.900.30 allows remote attackers to have unspecified impact via a crafted image.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3423
4605	CVE-2016-9559	MEDIUM	Medium	coders/tiff.c in ImageMagick before 7.0.3.7 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted image.	imagemagick	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3566
4606	CVE-2016-9557	MEDIUM	Medium	Integer overflow in jas_image.c in JasPer before 1.900.25 allows remote attackers to cause a denial of service (application crash) via a crafted file.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3670
4607	CVE-2016-9556	MEDIUM	Medium	A heap-buffer overflow vulnerability was found in ImageMagick in IsPixelGray function in pixel-accessor.h triggered by opening a malicious image.?	imagemagick	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3475
4608	CVE-2016-9555	HIGH	Critical	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data.	linux	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2749
4609	CVE-2016-9540	HIGH	Critical	tools/tiffcp.c in libtiff 4.0.6 has an out-of-bounds write on tiled images with odd tile width versus image width. Reported as MSVR 35103, aka cpStripToTile heap-buffer-overflow.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2399
4610	CVE-2016-9539	HIGH	Critical	tools/tiffcrop.c in libtiff 4.0.6 has an out-of-bounds read in readContigTilesIntoBuffer(). Reported as MSVR 35092.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2396
4611	CVE-2016-9538	HIGH	Critical	tools/tiffcrop.c in libtiff 4.0.6 reads an undefined buffer in readContigStripsIntoBuffer() because of a uint16 integer overflow. Reported as MSVR 35100.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2404
4612	CVE-2016-9537	HIGH	Critical	tools/tiffcrop.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in buffers. Reported as MSVR 35093, MSVR 35096, and MSVR 35097.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2405
4613	CVE-2016-9536	HIGH	Critical	tools/tiff2pdf.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers in t2p_process_jpeg_strip(). Reported as MSVR 35098, aka t2p_process_jpeg_strip heap-buffer-overflow.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2394
4614	CVE-2016-9535	HIGH	Critical	tif_predict.h and tif_predict.c in libtiff 4.0.6 have assertions that can lead to assertion failures in debug mode, or buffer overflows in release mode, when dealing with unusual tile size like YCbCr with subsampling. Reported as MSVR 35105, aka Predictor heap-buffer-overflow.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2393
4615	CVE-2016-9534	HIGH	Critical	tif_write.c in libtiff 4.0.6 has an issue in the error code path of TIFFFlushData1() that didn't reset the tif_rawcc and tif_rawcp members. Reported as MSVR 35095, aka TIFFFlushData1 heap-buffer-overflow.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2400
4616	CVE-2016-9533	HIGH	Critical	tif_pixarlog.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers. Reported as MSVR 35094, aka PixarLog horizontalDifference heap-buffer-overflow.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2401
4617	CVE-2016-9532	MEDIUM	Medium	Integer overflow in the writeBufferToSeparateStrips function in tiffcrop.c in LibTIFF before 4.0.7 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tif file.	libtiff	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3238

	A	B	C	D	E	F	G	H	I	J	K	L	M
4618	CVE-2016-9453	MEDIUM	High	The t2p_readwrite_pdf_image_tile function in LibTIFF allows remote attackers to cause a denial of service (out-of-bounds write and crash) or possibly execute arbitrary code via a JPEG file with a TIFFTAG_JPEGTABLES of length one.	libtiff	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3199
4619	CVE-2016-9448	MEDIUM	High	The TIFFFetchNormalTag function in LibTiff 4.0.6 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) by setting the tags TIFF_SETGET_C16ASCII or TIFF_SETGET_C32_ASCII to values that access 0-byte arrays. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9297.	libtiff	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3316
4620	CVE-2016-9447	MEDIUM	High	The ROM mappings in the NSF decoder in gstreamer 0.10.x allow remote attackers to cause a denial of service (out-of-bounds read or write) and possibly execute arbitrary code via a crafted NSF music file.	gstreamer	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-3204
4621	CVE-2016-9446	MEDIUM	High	The vmnc decoder in the gstreamer does not initialize the render canvas, which allows remote attackers to obtain sensitive information as demonstrated by thumbnailing a simple 1 frame vmnc movie that does not draw to the allocated render canvas.	gstreamer	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3189
4622	CVE-2016-9445	MEDIUM	High	Integer overflow in the vmnc decoder in the gstreamer allows remote attackers to cause a denial of service (crash) via large width and height values, which triggers a buffer overflow.	gstreamer	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3259
4623	CVE-2016-9444	MEDIUM	High	An unusually-formed DS record response could cause an assertion failure	bind	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2984
4624	CVE-2016-9427	HIGH	Critical	Integer overflow vulnerability in bdwgc before 2016-09-27 allows attackers to cause client of bdwgc denial of service (heap buffer overflow crash) and possibly execute arbitrary code via huge allocation.	bdwgc	Unchanged	8.0.0.14	9.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2786
4625	CVE-2016-9401	LOW	Medium	popd in bash might allow local users to bypass the restricted shell and cause a use-after-free via a crafted address.	bash	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3202
4626	CVE-2016-9399	MEDIUM	High	The calcstepsizes function in jpc_dec.c in JasPer 1.900.22 allows remote attackers to cause a denial of service (assertion failure) via unspecified vectors.CWE-617: Reachable Assertion	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3751
4627	CVE-2016-9398	MEDIUM	High	The jpc_floorlog2 function in jpc_math.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via unspecified vectors.CWE-617: Reachable Assertion	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3660
4628	CVE-2016-9397	MEDIUM	High	The jpc_dequantize function in jpc_dec.c in JasPer 1.900.13 allows remote attackers to cause a denial of service (assertion failure) via unspecified vectors.CWE-617: Reachable Assertion	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3795
4629	CVE-2016-9396	MEDIUM	High	The JPC_NOMINALGAIN function in jpc_t1cod.c in JasPer before 1.900.12 allows remote attackers to cause a denial of service (assertion failure) via unspecified vectors.CWE-617: Reachable Assertion	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3782
4630	CVE-2016-9395	MEDIUM	Medium	The jas_seq2d_create function in jas_seq.c in JasPer before 1.900.25 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3693
4631	CVE-2016-9394	MEDIUM	Medium	The jas_seq2d_create function in jas_seq.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3690
4632	CVE-2016-9393	MEDIUM	Medium	The jpc_pi_nextrpcl function in jpc_t2cod.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.CWE-617: Reachable Assertion	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3711
4633	CVE-2016-9392	MEDIUM	Medium	The calcstepsizes function in jpc_dec.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.CWE-617: Reachable Assertion	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3638
4634	CVE-2016-9391	MEDIUM	High	The jpc_bitstream_getbits function in jpc_bs.c in JasPer before 2.0.10 allows remote attackers to cause a denial of service (assertion failure) via a very large integer.CWE-617: Reachable Assertion	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3727
4635	CVE-2016-9390	MEDIUM	Medium	The jas_seq2d_create function in jas_seq.c in JasPer before 1.900.14 allows remote attackers to cause a denial of service (assertion failure) via a crafted image file.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3743
4636	CVE-2016-9389	MEDIUM	High	The jpc_irct and jpc_iict functions in jpc_mct.c in JasPer before 1.900.14 allow remote attackers to cause a denial of service (assertion failure).CWE-617: Reachable Assertion	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3650
4637	CVE-2016-9388	MEDIUM	Medium	The ras_getcmap function in ras_dec.c in JasPer before 1.900.14 allows remote attackers to cause a denial of service (assertion failure) via a crafted image file.CWE-617: Reachable Assertion	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3691
4638	CVE-2016-9387	MEDIUM	High	Integer overflow in the jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.13 allows remote attackers to have unspecified impact via a crafted file, which triggers an assertion failure.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3697
4639	CVE-2016-9381	MEDIUM	High	Race condition in QEMU in Xen allows local x86 HVM guest OS administrators to gain privileges by changing certain data on shared rings, aka a double fetch vulnerability.	qemu	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3277

	A	B	C	D	E	F	G	H	I	J	K	L	M
4640	CVE-2016-9376	MEDIUM	Medium	In Wireshark 2.2.0 to 2.2.1 and 2.0.0 to 2.0.7, the OpenFlow dissector could crash with memory exhaustion, triggered by network traffic or a capture file. This was addressed in epan/dissectors/packet-openflow_v5.c by ensuring that certain length values were sufficiently large.	wireshark	Unchanged	8.0.0.13	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2407
4641	CVE-2016-9375	MEDIUM	Medium	In Wireshark 2.2.0 to 2.2.1 and 2.0.0 to 2.0.7, the DTN dissector could go into an infinite loop, triggered by network traffic or a capture file. This was addressed in epan/dissectors/packet-dtn.c by checking whether SDNV evaluation was successful.	wireshark	Unchanged	8.0.0.13	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2406
4642	CVE-2016-9374	MEDIUM	Medium	In Wireshark 2.2.0 to 2.2.1 and 2.0.0 to 2.0.7, the AllJoyn dissector could crash with a buffer over-read, triggered by network traffic or a capture file. This was addressed in epan/dissectors/packet-alljoyn.c by ensuring that a length variable properly tracked the state of a signature variable.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2402
4643	CVE-2016-9373	MEDIUM	Medium	In Wireshark 2.2.0 to 2.2.1 and 2.0.0 to 2.0.7, the DCERPC dissector could crash with a use-after-free, triggered by network traffic or a capture file. This was addressed in epan/dissectors/packet-dcerpc-nt.c and epan/dissectors/packet-dcerpc-spoolss.c by using the wmem file scope for private strings.	wireshark	Unchanged	8.0.0.13	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2408
4644	CVE-2016-9372	MEDIUM	Medium	In Wireshark 2.2.0 to 2.2.1, the Profinet I/O dissector could loop excessively, triggered by network traffic or a capture file. This was addressed in plugins/profinet/packet-pn-rtc-one.c by rejecting input with too many I/O objects.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2398
4645	CVE-2016-9318	MEDIUM	High	libxml2 2.9.4 and earlier, as used in XMLSec 1.2.23 and earlier and other products, does not offer a flag directly indicating that the current document may be read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity (XXE) attacks via a crafted document.	libxml2	Unchanged	8.0.0.17	9.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2395
4646	CVE-2016-9317	HIGH	Medium	The gdImageCreate function in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (system hang) via an oversized image.	libgd	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3310
4647	CVE-2016-9313	HIGH	High	security/keys/big_key.c in the Linux kernel before 4.8.7 mishandles unsuccessful crypto registration in conjunction with successful key-type registration, which allows local users to cause a denial of service (NULL pointer dereference and panic) or possibly have unspecified other impact via a crafted application that uses the big_key data type.	linux	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2695
4648	CVE-2016-9312	MEDIUM	High	If a vulnerable instance of ntpd on Windows receives a crafted malicious packet that is "too big", ntpd will stop working.	ntp	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2335
4649	CVE-2016-9311	HIGH	Medium	If trap service, disabled by default, has been explicitly enabled, an attacker can send a specially crafted packet to cause a null pointer dereference that will crash ntpd, resulting in a denial of service.	ntp	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2321
4650	CVE-2016-9310	MEDIUM	Medium	An exploitable configuration modification vulnerability exists in the control mode (mode 6) functionality of ntpd. If, against long-standing BCP recommendations, "restrict default noquery ?" is not specified, a specially crafted control mode packet can set ntpd traps, providing information disclosure and DDoS amplification, and unset ntpd traps, disabling legitimate monitoring. A remote, unauthenticated, network attacker can trigger this vulnerability.	ntp	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2332
4651	CVE-2016-9298	MEDIUM	Medium	Heap overflow in the WaveletDenoiseImage function in MagickCore/fx.c in ImageMagick before 6.9.6-4 and 7.x before 7.0.3-6 allows remote attackers to cause a denial of service (crash) via a crafted image.	imagemagick	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3223
4652	CVE-2016-9297	MEDIUM	High	The TIFFFetchNormalTag function in LibTiff 4.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) via crafted TIFF_SETGET_C16ASCII or TIFF_SETGET_C32_ASCII tag values.	libtiff	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3235
4653	CVE-2016-9273	MEDIUM	Medium	tiffsplit in libtiff 4.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file, related to changing td_nstrips in TIFF_STRIPCHOP mode.	libtiff	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3265
4654	CVE-2016-9262	MEDIUM	Medium	Multiple integer overflows in the (1) jas_realloc function in base/jas_malloc.c and (2) mem_resize function in base/jas_stream.c in JasPer before 1.900.22 allow remote attackers to cause a denial of service via a crafted image, which triggers use after free vulnerabilities.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3738
4655	CVE-2016-9191	MEDIUM	Medium	The cgroup offline implementation in the Linux kernel through 4.8.11 mishandles certain drain operations, which allows local users to cause a denial of service (system hang) by leveraging access to a container environment for executing a crafted application, as demonstrated by trinity.	linux	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2690
4656	CVE-2016-9178	LOW	Medium	The __get_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel before 4.7.5 does not initialize a certain integer variable, which allows local users to obtain sensitive information from kernel stack memory by triggering failure of a get_user_ex call.	linux	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2708
4657	CVE-2016-9147	MEDIUM	High	An error handling a query response containing inconsistent DNSSEC information could cause an assertion failure	bind	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2962
4658	CVE-2016-9138	HIGH	Critical	PHP through 5.6.27 and 7.x through 7.0.12 mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup.	php	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2999

	A	B	C	D	E	F	G	H	I	J	K	L	M
4659	CVE-2016-9137	HIGH	Critical	Use-after-free vulnerability in the CURLFile implementation in ext/curl/curl_file.c in PHP before 5.6.27 and 7.x before 7.0.12 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that is mishandled during __wakeup processing.	php	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3009
4660	CVE-2016-9131	MEDIUM	High	A malformed response to an ANY query can cause an assertion failure during recursion	bind	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2980
4661	CVE-2016-9120	HIGH	High	Race condition in the ion_ioctl function in drivers/staging/android/ion/ion.c in the Linux kernel before 4.6 allows local users to gain privileges or cause a denial of service (use-after-free) by calling ION_IOC_FREE on two CPUs at the same time.	linux	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2739
4662	CVE-2016-9106	LOW	Medium	Memory leak in the v9fs_write function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) by leveraging failure to free an IO vector.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2719
4663	CVE-2016-9105	LOW	Medium	Memory leak in the v9fs_link function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via vectors involving a reference to the source fid object.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2721
4664	CVE-2016-9104	LOW	Medium	Multiple integer overflows in the (1) v9fs_xattr_read and (2) v9fs_xattr_write functions in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allow local guest OS administrators to cause a denial of service (QEMU process crash) via a crafted offset, which triggers an out-of-bounds access.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2685
4665	CVE-2016-9103	LOW	Medium	The v9fs_xattrcreate function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to obtain sensitive host heap memory information by reading xattribute values before writing to them.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2796
4666	CVE-2016-9102	LOW	Medium	Memory leak in the v9fs_xattrcreate function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption and QEMU process crash) via a large number of Txattrcreate messages with the same fid number.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2694
4667	CVE-2016-9101	LOW	Medium	Memory leak in hw/net/eepro100.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption and QEMU process crash) by repeatedly unplugging an i8255x (PRO100) NIC device.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2711
4668	CVE-2016-9085	HIGH	Critical	Multiple integer overflows in libwebp allows attackers to have unspecified impact via unknown vectors.	libwebp	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3222
4669	CVE-2016-9084	MEDIUM	High	drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows local users to cause a denial of service (integer overflow) or have unspecified other impact by leveraging access to a vfio PCI device file.	linux	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2743
4670	CVE-2016-9083	HIGH	High	drivers/vfio/pci/vfio_pci.c in the Linux kernel through 4.8.11 allows local users to bypass integer overflow checks, and cause a denial of service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file for a VFIO_DEVICE_SET_IRQS ioctl call, aka a state machine confusion bug.	linux	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2672
4671	CVE-2016-9082	MEDIUM	Medium	Integer overflow in the write_png function in cairo 1.14.6 allows remote attackers to cause a denial of service (invalid pointer dereference) via a large svg file.	cairo	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3282
4672	CVE-2016-9063	HIGH	CRITICAL	An integer overflow during the parsing of XML using the Expat library.	expat	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5036
4673	CVE-2016-9042	MEDIUM	MEDIUM	A vulnerability was found in NTP, affecting the origin timestamp check function. An attacker able to spoof messages from all of the configured peers could send crafted packets to ntpd, causing later replies from those peers to be discarded, resulting in denial of service.	ntp	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3625
4674	CVE-2016-9015	LOW	Low	Versions 1.17 and 1.18 of the Python urllib3 library suffer from a vulnerability that can cause them, in certain configurations, to not correctly validate TLS certificates. This places users of the library with those configurations at risk of man-in-the-middle and information leakage attacks. This vulnerability affects users using versions 1.17 and 1.18 of the urllib3 library, who are using the optional PyOpenSSL support for TLS instead of the regular standard library TLS backend, and who are using OpenSSL 1.1.0 via PyOpenSSL. This is an extremely uncommon configuration, so the security impact of this vulnerability is low.	python-urllib3	Unchanged	Not vulnerable	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3089
4675	CVE-2016-9011	MEDIUM	Medium	The wmf_malloc function in api.c in libwmf 0.2.8.4 allows remote attackers to cause a denial of service (application crash) via a crafted wmf file, which triggers a memory allocation failure.	libwmf	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3644
4676	CVE-2016-8910	LOW	Medium	The rtl8139_cplus_transmit function in hw/net/rtl8139.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) by leveraging failure to limit the ring descriptor count.CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')	qemu	Unchanged	8.0.0.12	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2170
4677	CVE-2016-8909	LOW	Medium	The intel_hda_xfer function in hw/audio/intel-hda.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) via an entry with the same value for buffer length and pointer position.CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')	qemu	Unchanged	8.0.0.12	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2175
4678	CVE-2016-8887	MEDIUM	Medium	The jp2_colr_destroy function in libjasper/jp2/jp2_cod.c in JasPer before 1.900.10 allows remote attackers to cause a denial of service (NULL pointer dereference).	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3757

	A	B	C	D	E	F	G	H	I	J	K	L	M
4679	CVE-2016-8886	MEDIUM	High	The jas_malloc function in libjasper/base/jas_malloc.c in JasPer before 1.900.11 allows remote attackers to have unspecified impact via a crafted file, which triggers a memory allocation failure.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3800
4680	CVE-2016-8885	MEDIUM	Medium	The bmp_getdata function in libjasper/bmp/bmp_dec.c in JasPer before 1.900.9 allows remote attackers to cause a denial of service (NULL pointer dereference) by calling the imginfo command with a crafted BMP image.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3777
4681	CVE-2016-8884	MEDIUM	Medium	The bmp_getdata function in libjasper/bmp/bmp_dec.c in JasPer 1.900.5 allows remote attackers to cause a denial of service (NULL pointer dereference) by calling the imginfo command with a crafted BMP image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8690.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3895
4682	CVE-2016-8883	MEDIUM	Medium	The jpc_dec_tiledecode function in jpc_dec.c in JasPer before 1.900.8 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.	jasper	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3077
4683	CVE-2016-8882	MEDIUM	Medium	The jpc_dec_tilefini function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.8 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted file.	jasper	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3084
4684	CVE-2016-8866	MEDIUM	High	The AcquireMagickMemory function in MagickCore/memory.c in GraphicsMagick 7.0.3.3 before 7.0.3.8 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8862.	imagemagick	Unchanged	8.0.0.17	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3844
4685	CVE-2016-8864	MEDIUM	High	named in ISC BIND 9.x before 9.9.9-P4, 9.10.x before 9.10.4-P4, and 9.11.x before 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db.c and resolver.c.	bind	Unchanged	8.0.0.12	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2143
4686	CVE-2016-8863	HIGH	Critical	Heap-based buffer overflow in the create_url_list function in gena/gena_device.c in Portable UPnP SDK (aka libupnp) before 1.6.21 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a valid URI followed by an invalid one in the CALLBACK header of an SUBSCRIBE request.	libupnp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3569
4687	CVE-2016-8862	MEDIUM	High	The AcquireMagickMemory function in MagickCore/memory.c in GraphicsMagick before 7.0.3.3 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure.	imagemagick	Unchanged	Not vulnerable	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3842
4688	CVE-2016-8858	HIGH	High	A memory exhaustion issue in OpenSSH that can be triggered before user authentication was found. An unauthenticated attacker could consume approx. 400 MB of memory per each connection. The attacker could set up multiple such connections to run out of server?s memory.	openssh	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2006
4689	CVE-2016-8743	MEDIUM	High	It was discovered that the HTTP parser in httpd incorrectly allowed certain characters not permitted by the HTTP protocol specification to appear unencoded in HTTP request headers. If httpd was used in conjunction with a proxy or backend server that interpreted those characters differently, a remote attacker could possibly use this flaw to inject data into HTTP responses, resulting in proxy cache poisoning. could use this flaw to decrypt and modify session data using a padding oracle attack. could use this flaw to decrypt and modify session data using a padding oracle attack.	apache	Unchanged	8.0.0.19	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3987
4690	CVE-2016-8740	MEDIUM	High	The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2678
4691	CVE-2016-8734	MEDIUM	Medium	Subversion's mod_dontdothat module and HTTP clients 1.4.0 through 1.8.16, and 1.9.0 through 1.9.4 are vulnerable to a denial-of-service attack caused by exponential XML entity expansion. The attack can cause the targeted process to consume an excessive amount of CPU resources or memory.	subversion	Unchanged	8.0.0.25	9.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5705
4692	CVE-2016-8707	MEDIUM	High	An exploitable out of bounds write exists in the handling of compressed TIFF images in ImageMagicks's convert utility. A crafted TIFF document can lead to an out of bounds write which in particular circumstances could be leveraged into remote code execution. The vulnerability can be triggered through any user controlled TIFF that is handled by this functionality.	imagemagick	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2867
4693	CVE-2016-8706	MEDIUM	High	An integer overflow in process_bin_sasl_auth function in Memcached, which is responsible for authentication commands of Memcached binary protocol, can be abused to cause heap overflow and lead to remote code execution.	memcached	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2996
4694	CVE-2016-8705	HIGH	Critical	Multiple integer overflows in process_bin_update function in Memcached, which is responsible for processing multiple commands of Memcached binary protocol, can be abused to cause heap overflow and lead to remote code execution.	memcached	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2976
4695	CVE-2016-8704	HIGH	Critical	An integer overflow in the process_bin_append_prepend function in Memcached, which is responsible for processing multiple commands of Memcached binary protocol, can be abused to cause heap overflow and lead to remote code execution.	memcached	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2986
4696	CVE-2016-8693	MEDIUM	High	Double free vulnerability in the mem_close function in jas_stream.c in JasPer before 1.900.10 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted BMP image to the imginfo command.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3419

	A	B	C	D	E	F	G	H	I	J	K	L	M
4697	CVE-2016-8692	MEDIUM	Medium	The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted YRsiz value in a BMP image to the imginfo command.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3406
4698	CVE-2016-8691	MEDIUM	Medium	The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted XRsiz value in a BMP image to the imginfo command.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3380
4699	CVE-2016-8690	MEDIUM	Medium	The bmp_getdata function in libjasper/bmp/bmp_dec.c in JasPer before 1.900.5 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted BMP image in an imginfo command.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3403
4700	CVE-2016-8689	MEDIUM	High	The read_Header function in archive_read_support_format_7zip.c in libarchive 3.2.1 allows remote attackers to cause a denial of service (out-of-bounds read) via multiple EmptyStream attributes in a header in a 7zip archive.	libarchive	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3418
4701	CVE-2016-8688	MEDIUM	Medium	The mtree bidder in libarchive 3.2.1 does not keep track of line sizes when extending the read-ahead, which allows remote attackers to cause a denial of service (crash) via a crafted file, which triggers an invalid read in the (1) detect_form or (2) bid_entry function in libarchive/archive_read_support_format_mtree.c.	libarchive	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3422
4702	CVE-2016-8687	MEDIUM	High	Stack-based buffer overflow in the safe_fprintf function in tar/util.c in libarchive 3.2.1 allows remote attackers to cause a denial of service via a crafted non-printable multibyte character in a filename.	libarchive	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3428
4703	CVE-2016-8678	MEDIUM	Medium	The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted file. NOTE: the vendor says This is a Q64 issue and we do not support Q64.	imagemagick	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3411
4704	CVE-2016-8677	MEDIUM	High	The AcquireQuantumPixels function in MagickCore/quantum.c in ImageMagick before 7.0.3-1 allows remote attackers to have unspecified impact via a crafted image file, which triggers a memory allocation failure.	imagemagick	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3383
4705	CVE-2016-8676	MEDIUM	Medium	The get_vlc2 function in get_bits.h in Libav 11.9 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted mp3 file. NOTE: this issue exists due to an incomplete fix for CVE-2016-8675.	libav	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3415
4706	CVE-2016-8675	MEDIUM	Medium	The get_vlc2 function in get_bits.h in Libav before 11.9 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted mp3 file, possibly related to startcode sequences during m4v detection.	libav	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3424
4707	CVE-2016-8670	HIGH	Critical	Integer signedness error in the dynamicGetbuf function in gd_io_dp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted imagecreatefromstring call.	libgd	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2959
4708	CVE-2016-8669	LOW	Medium	The serial_update_parameters function in hw/char/serial.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (divide-by-zero error and QEMU process crash) via vectors involving a value of divider greater than baud base.	qemu	Unchanged	8.0.0.12	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2176
4709	CVE-2016-8668	LOW	Medium	The rocker_io_writel function in hw/net/rocker/rocker.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of-bounds read and QEMU process crash) by leveraging failure to limit DMA buffer size.	qemu	Unchanged	8.0.0.12	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2173
4710	CVE-2016-8667	LOW	Medium	The rc4030_write function in hw/dma/rc4030.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (divide-by-zero error and QEMU process crash) via a large interval timer reload value.	qemu	Unchanged	8.0.0.12	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2178
4711	CVE-2016-8666	HIGH	High	The IP stack in the Linux kernel before 4.6 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for packets with tunnel stacking, as demonstrated by interleaved IPv4 headers and GRE headers, a related issue to CVE-2016-7039.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1828
4712	CVE-2016-8660	MEDIUM	Medium	The XFS subsystem in the Linux kernel through 4.8.2 allows local users to cause a denial of service (fdatasync failure and system hang) by using the vfs syscall group in the trinity program, related to a page lock order bug in the XFS seek hole/data implementation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1835
4713	CVE-2016-8658	MEDIUM	Medium	Stack-based buffer overflow in the brcmf_cfg80211_start_ap function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.7.5 allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a long SSID Information Element in a command to a Netlink socket.	linux	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1834
4714	CVE-2016-8655	HIGH	High	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packet_set_ring and packet_setsockopt functions.	linux	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2536
4715	CVE-2016-8650	MEDIUM	Medium	The mpi_powm function in lib/mpi/mpi-pow.c in the Linux kernel through 4.8.11 does not ensure that memory is allocated for limb data, which allows local users to cause a denial of service (stack memory corruption and panic) via an add_key system call for an RSA key with a zero exponent.	linux	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2675

	A	B	C	D	E	F	G	H	I	J	K	L	M
4716	CVE-2016-8649	HIGH	Critical	lxc-attach in LXC before 1.0.9 and 2.x before 2.0.6 allows an attacker inside of an unprivileged container to use an inherited file descriptor, of the host's /proc, to access the rest of the host's filesystem via the openat() family of syscalls.	lxc	Unchanged	Not vulnerable	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4220
4717	CVE-2016-8646	MEDIUM	Medium	The hash_accept function in crypto/algif_hash.c in the Linux kernel before 4.3.6 allows local users to cause a denial of service (OOPS) by attempting to trigger use of in-kernel hash algorithms for a socket that has received zero bytes of data.	linux	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2788
4718	CVE-2016-8645	MEDIUM	Medium	It was discovered that the Linux kernel, from at least v4.0 until v4.9-rc1, can hit BUG() statement in tcp_collapse() function after making a number of certain syscalls leading to a possible system crash.	linux	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2278
4719	CVE-2016-8637	LOW	HIGH	A local information disclosure issue was found in dracut before 045 when generating initramfs images with world-readable permissions when 'early cpio' is used, such as when including microcode updates. Local attacker can use this to obtain sensitive information from these files, such as encryption keys or credentials.	dracut	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4541
4720	CVE-2016-8636	HIGH	High	Integer overflow in the mem_check_range function in drivers/infiniband/sw/rxe/rxe_mr.c in the Linux kernel before 4.9.10 allows local users to cause a denial of service (memory corruption), obtain sensitive information from kernel memory, or possibly have unspecified other impact via a write or read request involving the RDMA protocol over infiniband (aka Soft RoCE) technology.	linux	Unchanged	Not vulnerable	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3392
4721	CVE-2016-8635	MEDIUM	MEDIUM	It was found that Diffie Hellman Client key exchange handling in NSS 3.21.x was vulnerable to small subgroup confinement attack. An attacker could use this flaw to recover private keys by confining the client DH key to small subgroup of the desired group.	nss	Unchanged	Not vulnerable	9.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4536
4722	CVE-2016-8633	MEDIUM	Medium	drivers/firewire/net.c in the Linux kernel before 4.8.7, in certain unusual hardware configurations, allows remote attackers to execute arbitrary code via crafted fragmented packets.	linux	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2763
4723	CVE-2016-8632	HIGH	High	The tipc_msg_build function in net/tipc/msg.c in the Linux kernel through 4.8.11 does not validate the relationship between the minimum fragment length and the maximum packet size, which allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) by leveraging the CAP_NET_ADMIN capability.	linux	Unchanged	8.0.0.14	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2798
4724	CVE-2016-8630	MEDIUM	Medium	The x86_decode_insn function in arch/x86/kvm/emulate.c in the Linux kernel before 4.8.7, when KVM is enabled, allows local users to cause a denial of service (host OS crash) via a certain use of a ModR/M byte in an undefined instruction.	linux	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2715
4725	CVE-2016-8626	MEDIUM	MEDIUM	A flaw was found in Red Hat Ceph before 0.94.9-8. The way Ceph Object Gateway handles POST object requests permits an authenticated attacker to launch a denial of service attack by sending null or specially crafted POST object requests.	ceph	Unchanged	8.0.0.27	9.0.0.18	Won't Fix	10.18.44.1	Not vulnerable	Not vulnerable	LIN10-4535
4726	CVE-2016-8625	MEDIUM	HIGH	When curl is built with libidn to handle International Domain Names (IDNA), it translates them to puny code for DNS resolving using the IDNA 2003 standard, while IDNA 2008 is the modern and up-to-date IDNA standard. Have security implications if you for example use an URL parser that follows the RFC to check for allowed domains before using curl to request them. Variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer. function is also used internally when parsing for example HTTP cookies (possibly received from remote servers) and it can be used when doing conditional HTTP requests. Or with [a-z], using letters.	curl	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1917
4727	CVE-2016-8624	MEDIUM	HIGH	curl doesn't parse the authority component of the URL correctly when the host name part ends with a '#' character, and could instead be tricked into connecting to a different host. This may have security implications if you for example use an URL parser that follows the RFC to check for allowed domains before using curl to request them. Variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer. function is also used internally when parsing for example HTTP cookies (possibly received from remote servers) and it can be used when doing conditional HTTP requests. Or with [a-z], using letters.	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1916
4728	CVE-2016-8623	MEDIUM	HIGH	libcurl explicitly allows users to share cookies between multiple easy handles that are concurrently employed by different threads. Would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer. function is also used internally when parsing for example HTTP cookies (possibly received from remote servers) and it can be used when doing conditional HTTP requests. Or with [a-z], using letters.	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1915

	A	B	C	D	E	F	G	H	I	J	K	L	M
4729	CVE-2016-8622	HIGH	CRITICAL	The URL percent-encoding decode function in libcurl is called `curl_easy_unescape`. Internally, even if this function would be made to allocate a unscape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer. function is also used internally when parsing for example HTTP cookies (possibly received from remote servers) and it can be used when doing conditional HTTP requests. Or with [a-z], using letters.	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1912
4730	CVE-2016-8621	MEDIUM	HIGH	The `curl_getdate` converts a given date string into a numerical timestamp and it supports a range of different formats and possibilities to express a date and time. The underlying date parsing function is also used internally when parsing for example HTTP cookies (possibly received from remote servers) and it can be used when doing conditional HTTP requests. Or with [a-z], using letters.	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1911
4731	CVE-2016-8620	HIGH	CRITICAL	The curl tool's "globbing" feature allows a user to specify a numerical range through which curl will iterate. It is typically specified as [1-5], specifying the first and the last numbers in the range. Or with [a-z], using letters.	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1919
4732	CVE-2016-8619	HIGH	CRITICAL	In curl's implementation of the Kerberos authentication mechanism, the function `read_data()` in security.c is used to fill the necessary krb5 structures. When reading one of the length fields from the socket, it fails to ensure that the length parameter passed to realloc() is not set to 0. used internallty in numerous situations.	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1910
4733	CVE-2016-8618	HIGH	CRITICAL	The libcurl API function called `curl_maprintf()` can be tricked into doing a double-free due to an unsafe `size_t` multiplication, on systems using 32 bit `size_t` variables. The function is also used internallty in numerous situations.	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1908
4734	CVE-2016-8617	MEDIUM	HIGH	In libcurl's base64 encode function, the output buffer is allocated as follows without any checks on insize	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1907
4735	CVE-2016-8616	MEDIUM	MEDIUM	When re-using a connection, curl was doing case insensitive comparisons of user name and password with the existing connections.	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1906
4736	CVE-2016-8615	MEDIUM	HIGH	If cookie state is written into a cookie jar file that is later read back and used for subsequent requests, a malicious HTTP server can inject new cookies for arbitrary domains into said cookie jar.	curl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1904
4737	CVE-2016-8612	LOW	MEDIUM	Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.	apache	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3569
4738	CVE-2016-8610	MEDIUM	High	A denial of service flaw was found in the way the SSL/TLS protocol, defined processing of ALERT packets during an SSL handshake. An attacker could use this flaw to DoS servers compiled against cryptographic libraries, which do not allocate an extra thread to process ClientHello packets.	openssl	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1846
4739	CVE-2016-8606	HIGH	Critical	The REPL server (--listen) in GNU Guile 2.0.12 allows an attacker to execute arbitrary code via an HTTP inter-protocol attack.	guile	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3076
4740	CVE-2016-8602	MEDIUM	High	The .sethalftone5 function in psi/zht2.c in Ghostscript before 9.21 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted Postscript document that calls .sethalftone5 with an empty operand stack.	ghostscript	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4022
4741	CVE-2016-8595	MEDIUM	Medium	The gsm_parse function in libavcodec/gsm_parser.c in FFmpeg before 3.1.5 allows remote attackers to cause a denial of service (assert fault) via a crafted AVI file.	gst-ffmpeg	Unchanged	Won't Fix	9.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2866
4742	CVE-2016-8578	LOW	Medium	The v9fs_iov_vunmarshal function in fsdev/9p-iov-marshal.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) by sending an empty string parameter to a 9P operation.	qemu	Unchanged	8.0.0.12	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2160
4743	CVE-2016-8577	LOW	Medium	Memory leak in the v9fs_read function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via vectors related to an I/O read operation.	qemu	Unchanged	8.0.0.12	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2146
4744	CVE-2016-8576	LOW	Medium	The xhci_ring_fetch function in hw/usb/hcd-xhci.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by leveraging failure to limit the number of link Transfer Request Blocks (TRB) to process.CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')	qemu	Unchanged	8.0.0.12	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2163
4745	CVE-2016-8575	HIGH	Critical	The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2017-5482.	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3281
4746	CVE-2016-8574	HIGH	Critical	The FRF.15 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:frf15_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3278
4747	CVE-2016-8569	MEDIUM	Medium	The git_oid_nfmt function in commit.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (NULL pointer dereference) via a cat-file command with a crafted object file.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3286
4748	CVE-2016-8568	MEDIUM	Medium	The git_commit_message function in oid.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a cat-file command with a crafted object file.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3302

	A	B	C	D	E	F	G	H	I	J	K	L	M
4749	CVE-2016-8405	MEDIUM	Medium	An information disclosure vulnerability in kernel components including the ION subsystem, Binder, USB driver and networking subsystem could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31651010.	linux	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4180
4750	CVE-2016-8399	HIGH	High	An elevation of privilege vulnerability in the kernel networking subsystem could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Moderate because it first requires compromising a privileged process and current compiler optimizations restrict access to the vulnerable code. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31349935.	linux	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4216
4751	CVE-2016-8339	HIGH	Critical	A buffer overflow in Redis 3.2.x prior to 3.2.4 causes arbitrary code execution when a crafted command is sent. An out of bounds write vulnerability exists in the handling of the client-output-buffer-limit option during the CONFIG SET command for the Redis data structure store. A crafted CONFIG SET command can lead to an out of bounds write potentially resulting in code execution.	redis	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2166
4752	CVE-2016-8331	MEDIUM	High	An exploitable remote code execution vulnerability exists in the handling of TIFF images in LibTIFF version 4.0.6. A crafted TIFF document can lead to a type confusion vulnerability resulting in remote code execution. This vulnerability can be triggered via a TIFF file delivered to the application using LibTIFF's tag extension functionality.CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')	tiff	Unchanged	Investigate	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2162
4753	CVE-2016-8328	MEDIUM	Low	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Java Mission Control). The supported version that is affected is Java SE: 8u112. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: Applies to Java Mission Control Installation. CVSS v3.0 Base Score 3.7 (Integrity impacts).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3254
4754	CVE-2016-8327	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.4 (Availability impacts).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3253
4755	CVE-2016-8318	LOW	Medium	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.8 (Availability impacts).	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3304
4756	CVE-2016-8290	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Performance Schema, a different vulnerability than CVE-2016-5633.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2161
4757	CVE-2016-8289	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows local users to affect integrity and availability via vectors related to Server: InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2159
4758	CVE-2016-8288	MEDIUM	Low	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect integrity via vectors related to Server: InnoDB Plugin.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2150
4759	CVE-2016-8287	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2177
4760	CVE-2016-8286	LOW	Low	Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows remote authenticated users to affect confidentiality via vectors related to Server: Security: Privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2155
4761	CVE-2016-8284	LOW	Low	Unspecified vulnerability in Oracle MySQL 5.6.31 and earlier and 5.7.13 and earlier allows local users to affect availability via vectors related to Server: Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2158
4762	CVE-2016-8283	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to Server: Types.	mysql	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2183
4763	CVE-2016-7995	LOW	Medium	Memory leak in the ehci_process_itd function in hw/usb/hcd-ehci.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via a large number of crafted buffer page select (PG) indexes.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2723

	A	B	C	D	E	F	G	H	I	J	K	L	M
4764	CVE-2016-7994	LOW	Medium	Memory leak in the virtio_gpu_resource_create_2d function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_CREATE_2D commands.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2732
4765	CVE-2016-7993	HIGH	Critical	A bug in util-print.c:relts_print() in tcpdump before 4.9.0 could cause a buffer overflow in multiple protocol parsers (DNS, DVMRP, HSRP, IGMP, lightweight resolver protocol, PIM).	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3173
4766	CVE-2016-7992	HIGH	Critical	The Classical IP over ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-cip.c:cip_if_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3300
4767	CVE-2016-7986	HIGH	Critical	The GeoNetworking parser in tcpdump before 4.9.0 has a buffer overflow in print-geonet.c, multiple functions.	tcpdump	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3307
4768	CVE-2016-7985	HIGH	Critical	The CALM FAST parser in tcpdump before 4.9.0 has a buffer overflow in print-calm-fast.c:calm_fast_print().	tcpdump	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3293
4769	CVE-2016-7984	HIGH	Critical	The TFTP parser in tcpdump before 4.9.0 has a buffer overflow in print-tftp.c:tftp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3250
4770	CVE-2016-7983	HIGH	Critical	The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3261
4771	CVE-2016-7979	HIGH	Critical	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently execute arbitrary code by leveraging type confusion in .initialize_dsc_parser.	ghostscript	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4278
4772	CVE-2016-7978	HIGH	Critical	Use-after-free vulnerability in Ghostscript 9.20 might allow remote attackers to execute arbitrary code via vectors related to a reference leak in .setdevice.	ghostscript	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4287
4773	CVE-2016-7977	MEDIUM	Medium	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently read arbitrary files via the use of the .libfile operator in a crafted postscript document.	ghostscript	Unchanged	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4290
4774	CVE-2016-7976	MEDIUM	High	The PS Interpreter in Ghostscript 9.18 and 9.20 allows remote attackers to execute arbitrary code via crafted userparams.	ghostscript	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4979
4775	CVE-2016-7975	HIGH	Critical	The TCP parser in tcpdump before 4.9.0 has a buffer overflow in print-tcp.c:tcp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3168
4776	CVE-2016-7974	HIGH	Critical	The IP parser in tcpdump before 4.9.0 has a buffer overflow in print-ip.c, multiple functions.	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3162
4777	CVE-2016-7973	HIGH	Critical	The AppleTalk parser in tcpdump before 4.9.0 has a buffer overflow in print-atalk.c, multiple functions.	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3268
4778	CVE-2016-7972	MEDIUM	High	The check_allocations function in libass/ass_shaper.c in libass before 0.13.4 allows remote attackers to cause a denial of service (memory allocation failure) via unspecified vectors.	libass	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3582
4779	CVE-2016-7970	MEDIUM	High	Buffer overflow in the calc_coeff function in libass/ass_blur.c in libass before 0.13.4 allows remote attackers to cause a denial of service via unspecified vectors.	libass	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3558
4780	CVE-2016-7969	MEDIUM	High	The wrap_lines_smart function in ass_render.c in libass before 0.13.4 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors, related to 0/3 line wrapping equalization.	libass	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3561
4781	CVE-2016-7958	MEDIUM	High	In Wireshark 2.2.0, the NCP dissector could crash, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/CMakeLists.txt by registering this dissector.	wireshark	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4142
4782	CVE-2016-7957	MEDIUM	High	In Wireshark 2.2.0, the Bluetooth L2CAP dissector could crash, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-btl2cap.c by avoiding use of a seven-byte memcmp for potentially shorter strings.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4071
4783	CVE-2016-7953	HIGH	Critical	Buffer underflow in X.org libXvMC before 1.0.10 allows remote X servers to have unspecified impact via an empty string.	libxvmc	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2686
4784	CVE-2016-7952	MEDIUM	High	X.org libXtst before 1.2.3 allows remote X servers to cause a denial of service (infinite loop) via a reply in the (1) XRecordStartOfData, (2) XRecordEndOfData, or (3) XRecordClientDied category without a client sequence and with attached data.	libxtst	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2700
4785	CVE-2016-7951	HIGH	Critical	Multiple integer overflows in X.org libXtst before 1.2.3 allow remote X servers to trigger out-of-bounds memory access operations by leveraging the lack of range checks.	libxtst	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2667
4786	CVE-2016-7950	HIGH	Critical	The XRenderQueryFilters function in X.org libXrender before 0.9.10 allows remote X servers to trigger out-of-bounds write operations via vectors involving filter name lengths.	libxrender	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2755
4787	CVE-2016-7949	HIGH	Critical	Multiple buffer overflows in the (1) XvQueryAdaptors and (2) XvQueryEncodings functions in X.org libXrender before 0.9.10 allow remote X servers to trigger out-of-bounds write operations via vectors involving length fields.	libxrender	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2680
4788	CVE-2016-7948	HIGH	Critical	X.org libXrandr before 1.5.1 allows remote X servers to trigger out-of-bounds write operations by leveraging mishandling of reply data.	libxrandr	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2712
4789	CVE-2016-7947	HIGH	Critical	Multiple integer overflows in X.org libXrandr before 1.5.1 allow remote X servers to trigger out-of-bounds write operations via a crafted response.	libxrandr	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2740
4790	CVE-2016-7946	MEDIUM	High	X.org libXi before 1.7.7 allows remote X servers to cause a denial of service (infinite loop) via vectors involving length fields.	libxi	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2682
4791	CVE-2016-7945	MEDIUM	High	Multiple integer overflows in X.org libXi before 1.7.7 allow remote X servers to cause a denial of service (out-of-bounds memory access or infinite loop) via vectors involving length fields.	libxi	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2684
4792	CVE-2016-7944	HIGH	Critical	Integer overflow in X.org libXfixes before 5.0.3 on 32-bit platforms might allow remote X servers to gain privileges via a length value of INT_MAX, which triggers the client to stop reading data and get out of sync.	libxfixes	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2757
4793	CVE-2016-7943	HIGH	Critical	The XListFonts function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving length fields, which trigger out-of-bounds write operations.	libx11	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2670

	A	B	C	D	E	F	G	H	I	J	K	L	M
4794	CVE-2016-7942	HIGH	Critical	The XGetImage function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving image type and geometry, which triggers out-of-bounds read operations.	libx11	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2785
4795	CVE-2016-7940	HIGH	Critical	The STP parser in tcpdump before 4.9.0 has a buffer overflow in print-stp.c, multiple functions.	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3296
4796	CVE-2016-7939	HIGH	Critical	The GRE parser in tcpdump before 4.9.0 has a buffer overflow in print-gre.c, multiple functions.	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3158
4797	CVE-2016-7938	HIGH	Critical	The ZeroMQ parser in tcpdump before 4.9.0 has an integer overflow in print-zeromq.c:zmtp1_print_frame().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3169
4798	CVE-2016-7937	HIGH	Critical	The VAT parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:vat_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3176
4799	CVE-2016-7936	HIGH	Critical	The UDP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:udp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3200
4800	CVE-2016-7935	HIGH	Critical	The RTP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3257
4801	CVE-2016-7934	HIGH	Critical	The RTCP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtcp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3260
4802	CVE-2016-7933	HIGH	Critical	The PPP parser in tcpdump before 4.9.0 has a buffer overflow in print-ppp.c:ppp_hdlc_if_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3227
4803	CVE-2016-7932	HIGH	Critical	The PIM parser in tcpdump before 4.9.0 has a buffer overflow in print-pim.c:pimv2_check_checksum().	tcpdump	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3217
4804	CVE-2016-7931	HIGH	Critical	The MPLS parser in tcpdump before 4.9.0 has a buffer overflow in print-mpls.c:mpls_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3184
4805	CVE-2016-7930	HIGH	Critical	The LLC/SNAP parser in tcpdump before 4.9.0 has a buffer overflow in print-llc.c:llc_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3172
4806	CVE-2016-7929	HIGH	Critical	The Juniper PPPoE ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-juniper.c:juniper_parse_header().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3231
4807	CVE-2016-7928	HIGH	Critical	The IPComp parser in tcpdump before 4.9.0 has a buffer overflow in print-ipcomp.c:ipcomp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3303
4808	CVE-2016-7927	HIGH	Critical	The IEEE 802.11 parser in tcpdump before 4.9.0 has a buffer overflow in print-802_11.c:ieee802_11_radio_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3225
4809	CVE-2016-7926	HIGH	Critical	The Ethernet parser in tcpdump before 4.9.0 has a buffer overflow in print-ether.c:ethertype_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3216
4810	CVE-2016-7925	HIGH	Critical	The compressed SLIP parser in tcpdump before 4.9.0 has a buffer overflow in print-sl.c:sl_if_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3313
4811	CVE-2016-7924	HIGH	Critical	The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:oam_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3185
4812	CVE-2016-7923	HIGH	Critical	The ARP parser in tcpdump before 4.9.0 has a buffer overflow in print-arp.c:arp_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3262
4813	CVE-2016-7922	HIGH	Critical	The AH parser in tcpdump before 4.9.0 has a buffer overflow in print-ah.c:ah_print().	tcpdump	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3237
4814	CVE-2016-7917	MEDIUM	Medium	The nfnetlink_rcv_batch function in net/netfilter/nfnetlink.c in the Linux kernel before 4.5 does not check whether a batch message's length field is large enough, which allows local users to obtain sensitive information from kernel memory or cause a denial of service (infinite loop or out-of-bounds read) by leveraging the CAP_NET_ADMIN capability.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2268
4815	CVE-2016-7916	MEDIUM	Medium	Race condition in the environ_read function in fs/proc/base.c in the Linux kernel before 4.5.4 allows local users to obtain sensitive information from kernel memory by reading a /proc/*/environ file during a process-setup time interval in which environment-variable copying is incomplete.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2269
4816	CVE-2016-7915	MEDIUM	Medium	The hid_input_field function in drivers/hid/hid-core.c in the Linux kernel before 4.6 allows physically proximate attackers to obtain sensitive information from kernel memory or cause a denial of service (out-of-bounds read) by connecting a device, as demonstrated by a Logitech DJ receiver.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2271
4817	CVE-2016-7914	HIGH	Medium	The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.5.3 does not check whether a slot is a leaf, which allows local users to obtain sensitive information from kernel memory or cause a denial of service (invalid pointer dereference and out-of-bounds read) via an application that uses associative-array data structures, as demonstrated by the keyutils test suite.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2272
4818	CVE-2016-7913	HIGH	High	The xc2028_set_config function in drivers/media/tuners/tuner-xc2028.c in the Linux kernel before 4.6 allows local users to gain privileges or cause a denial of service (use-after-free) via vectors involving omission of the firmware name from a certain data structure.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2275
4819	CVE-2016-7912	HIGH	High	Use-after-free vulnerability in the ffs_user_copy_worker function in drivers/usb/gadget/function/f_fs.c in the Linux kernel before 4.5.3 allows local users to gain privileges by accessing an I/O data structure after a certain callback call.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2276
4820	CVE-2016-7911	HIGH	High	Race condition in the get_task_ioprio function in block/ioprio.c in the Linux kernel before 4.6.6 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted ioprio_get system call.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2277
4821	CVE-2016-7910	HIGH	High	Use-after-free vulnerability in the disk_seqf_stop function in block/genhd.c in the Linux kernel before 4.7.1 allows local users to gain privileges by leveraging the execution of a certain stop operation even if the corresponding start operation had failed.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2263
4822	CVE-2016-7909	MEDIUM	Medium	The pcnet_rdra_addr function in hw/net/pcnet.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by setting the (1) receive or (2) transmit descriptor ring length to 0.	qemu	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1713

	A	B	C	D	E	F	G	H	I	J	K	L	M
4823	CVE-2016-7908	LOW	Medium	The mcf_fec_do_tx function in hw/net/mcf_fec.c in QEMU (aka Quick Emulator) does not properly limit the buffer descriptor count when transmitting packets, which allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via vectors involving a buffer descriptor with a length of 0 and crafted values in bd.flags.	qemu	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1716
4824	CVE-2016-7907	LOW	Medium	The imx_fec_do_tx function in hw/net/imx_fec.c in QEMU (aka Quick Emulator) does not properly limit the buffer descriptor count when transmitting packets, which allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via vectors involving a buffer descriptor with a length of 0 and crafted values in bd.flags.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1743
4825	CVE-2016-7906	MEDIUM	Medium	magick/attribute.c in ImageMagick 7.0.3-2 allows remote attackers to cause a denial of service (use-after-free) via a crafted file.	imagemagick	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3171
4826	CVE-2016-7905	MEDIUM	Medium	The read_gab2_sub function in libavformat/avidec.c in FFmpeg before 3.1.4 allows remote attackers to cause a denial of service (NULL pointer used) via a crafted AVI file.	gst-ffmpeg	Unchanged	Won't Fix	9.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2879
4827	CVE-2016-7837	MEDIUM	High	Buffer overflow in BlueZ 5.41 and earlier allows an attacker to execute arbitrary code via the parse_line function used in some userland utilities.	bluez	Unchanged	8.0.0.30	9.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4400
4828	CVE-2016-7799	MEDIUM	Medium	MagickCore/profile.c in ImageMagick before 7.0.3-2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	imagemagick	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3196
4829	CVE-2016-7798	MEDIUM	High	The openssl gem for Ruby uses the same initialization vector (IV) in GCM Mode (aes-*-gcm) when the IV is set before the key, which makes it easier for context-dependent attackers to bypass the encryption protection mechanism.	openssl	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3292
4830	CVE-2016-7797	MEDIUM	High	Pacemaker before 1.1.15, when using pacemaker remote, might allow remote attackers to cause a denial of service (node disconnection) via an unauthenticated connection.	pacemaker	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3783
4831	CVE-2016-7796	MEDIUM	Medium	It was found that systemd fails an assertion in manager_invoke_notify_message() when a zero-length message is received over its notification socket, causing it to no longer perform it's expected functionality. This issue was assigned CVE-2016-7795 and is tracked via bug 1380286	systemd	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1750
4832	CVE-2016-7795	MEDIUM	Medium	It was found that systemd fails an assertion in manager_invoke_notify_message when a zero-length message is received over its notification socket. After failing the assertion, PID 1 hangs in the pause system call, making no longer possible to start and stop daemons or cleanly reboot the system. Inetd-style services managed by systemd no longer accept connections.	systemd	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1668
4833	CVE-2016-7785	MEDIUM	Medium	The avi_read_seek function in libavformat/avidec.c in FFmpeg before 3.1.4 allows remote attackers to cause a denial of service (assert fault) via a crafted AVI file.	gst-ffmpeg	Unchanged	Won't Fix	9.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2872
4834	CVE-2016-7568	HIGH	Critical	Integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP through 7.0.11, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted imagewebp and imagedestroy calls.	gd	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1754
4835	CVE-2016-7562	MEDIUM	Medium	The ff_draw_pc_font function in libavcodec/cga_data.c in FFmpeg before 3.1.4 allows remote attackers to cause a denial of service (buffer overflow) via a crafted AVI file.	gst-ffmpeg	Unchanged	Won't Fix	9.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2885
4836	CVE-2016-7555	MEDIUM	Medium	The avi_read_header function in libavformat/avidec.c in FFmpeg before 3.1.4 is vulnerable to memory leak when decoding an AVI file that has a crafted strh structure.	gst-ffmpeg	Unchanged	Won't Fix	9.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2883
4837	CVE-2016-7543	HIGH	High	Bash before 4.4 allows local users to execute arbitrary commands with root privileges via crafted SHELLOPTS and PS4 environment variables.	bash	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3195
4838	CVE-2016-7540	MEDIUM	Medium	coders/rgf.c in ImageMagick before 6.9.4-10 allows remote attackers to cause a denial of service (assertion failure) by converting an image to rgf format.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4052
4839	CVE-2016-7539	HIGH	High	Memory leak in AcquireVirtualMemory in ImageMagick before 7 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.	imagemagick	Unchanged	8.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4813
4840	CVE-2016-7538	MEDIUM	Medium	coders/psd.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4106
4841	CVE-2016-7537	MEDIUM	Medium	MagickCore/memory.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted PDB file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4031
4842	CVE-2016-7536	MEDIUM	Medium	magick/profile.c in ImageMagick allows remote attackers to cause a denial of service (segmentation fault) via a crafted profile.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4043
4843	CVE-2016-7535	MEDIUM	Medium	coders/psd.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted PSD file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4144
4844	CVE-2016-7534	MEDIUM	Medium	The generic decoder in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4040
4845	CVE-2016-7533	MEDIUM	Medium	The ReadWPGImage function in coders/wpg.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WPG file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4039
4846	CVE-2016-7531	MEDIUM	Medium	MagickCore/memory.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted PDB file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4125
4847	CVE-2016-7530	MEDIUM	Medium	The quantum handling code in ImageMagick allows remote attackers to cause a denial of service (divide-by-zero error or out-of-bounds write) via a crafted file.	imagemagick	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4146

	A	B	C	D	E	F	G	H	I	J	K	L	M
4848	CVE-2016-7529	MEDIUM	Medium	coders/xcf.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted XCF file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4147
4849	CVE-2016-7528	MEDIUM	Medium	The ReadVIFFImage function in coders/viff.c in ImageMagick allows remote attackers to cause a denial of service (segmentation fault) via a crafted VIFF file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4021
4850	CVE-2016-7527	MEDIUM	Medium	coders/wpg.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4010
4851	CVE-2016-7526	MEDIUM	Medium	coders/wpg.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4051
4852	CVE-2016-7525	MEDIUM	Medium	Heap-based buffer overflow in coders/psd.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PSD file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4041
4853	CVE-2016-7524	MEDIUM	MEDIUM	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	imagemagick	Unchanged	Investigate	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4033
4854	CVE-2016-7523	MEDIUM	MEDIUM	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	imagemagick	Unchanged	Investigate	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-4034
4855	CVE-2016-7522	MEDIUM	Medium	The ReadPSDImage function in MagickCore/locale.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PSD file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4138
4856	CVE-2016-7521	MEDIUM	Medium	Heap-based buffer overflow in coders/psd.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PSD file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4084
4857	CVE-2016-7520	MEDIUM	Medium	Heap-based buffer overflow in coders/hdr.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted HDR file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4093
4858	CVE-2016-7519	MEDIUM	Medium	The ReadRLEImage function in coders/rle.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4017
4859	CVE-2016-7518	MEDIUM	Medium	The ReadSUNImage function in coders/sun.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted SUN file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4075
4860	CVE-2016-7517	MEDIUM	Medium	The EncodeImage function in coders/pict.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PICT file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4062
4861	CVE-2016-7516	MEDIUM	Medium	The ReadVIFFImage function in coders/viff.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted VIFF file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4094
4862	CVE-2016-7515	MEDIUM	Medium	The ReadRLEImage function in coders/rle.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the number of pixels.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4036
4863	CVE-2016-7514	MEDIUM	Medium	The ReadPSDChannelPixels function in coders/psd.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PSD file.	imagemagick	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4097
4864	CVE-2016-7513	MEDIUM	Medium	Off-by-one error in magick/cache.c in ImageMagick allows remote attackers to cause a denial of service (segmentation fault) via unspecified vectors.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4018
4865	CVE-2016-7502	MEDIUM	High	The cavs_idct8_add_c function in libavcodec/cavsdsp.c in FFmpeg before 3.1.4 is vulnerable to reading out-of-bounds memory when decoding with cavs_decode.	gst-ffmpeg	Unchanged	Won't Fix	9.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2882
4866	CVE-2016-7499	MEDIUM	Medium	The sbr_make_f_master function in aacsbr.c in Libav 11.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted mp3 file.	libav	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3381
4867	CVE-2016-7480	HIGH	Critical	The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c in PHP before 7.0.12 does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2993
4868	CVE-2016-7479	HIGH	Critical	In all versions of PHP 7, during the unserialization process, resizing the 'properties' hash table of a serialized object may lead to use-after-free. A remote attacker may exploit this bug to gain arbitrary code execution.	php	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3080
4869	CVE-2016-7478	MEDIUM	High	Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876.	php	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2963
4870	CVE-2016-7477	MEDIUM	Medium	The ff_put_pixels8_xy2_mmx function in rnd_template.c in Libav 11.7 allows remote attackers to cause a denial of service (invalid memory access and crash) via a crafted mp3 file. NOTE: this issue was originally reported as involving a NULL pointer dereference.	libav	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3404
4871	CVE-2016-7466	LOW	Medium	Memory leak in the usb_xhci_exit function in hw/usb/hcd-xhci.c in QEMU (aka Quick Emulator), when the xhci uses msix, allows local guest OS administrators to cause a denial of service (memory consumption and possibly QEMU process crash) by repeatedly unplugging a USB device.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2673
4872	CVE-2016-7450	MEDIUM	High	The ff_log2_16bit_c function in libavutil/intmath.h in FFmpeg before 3.1.4 is vulnerable to reading out-of-bounds memory when it decodes a malformed AIFF file.	gst-ffmpeg	Unchanged	Won't Fix	9.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2868
4873	CVE-2016-7444	MEDIUM	High	The gnutls_ocsp_resp_check_crt function in lib/x509/ocsp.c in GnuTLS before 3.4.15 and 3.5.x before 3.5.4 does not verify the serial length of an OCSP response, which might allow remote attackers to bypass an intended certificate validation mechanism via vectors involving trailing bytes left by gnutls_malloc.	gnutls	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1735
4874	CVE-2016-7440	LOW	Medium	The C software implementation of AES Encryption and Decryption in wolfSSL (formerly CyaSSL) before 3.9.10 makes it easier for local users to discover AES keys by leveraging cache-bank timing differences.	wolfssl	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2747

	A	B	C	D	E	F	G	H	I	J	K	L	M
4875	CVE-2016-7439	LOW	Medium	The C software implementation of RSA in wolfSSL (formerly CyaSSL) before 3.9.10 makes it easier for local users to discover RSA keys by leveraging cache-bank hit differences.	wolfssl	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2769
4876	CVE-2016-7438	LOW	Medium	The C software implementation of ECC in wolfSSL (formerly CyaSSL) before 3.9.10 makes it easier for local users to discover RSA keys by leveraging cache-bank hit differences.	wolfssl	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2744
4877	CVE-2016-7434	MEDIUM	High	If ntpd is configured to allow mrulist query requests from a server that sends a crafted malicious packet, ntpd will crash on receipt of that crafted malicious mrulist query packet.	ntp	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2337
4878	CVE-2016-7433	MEDIUM	Medium	Bug 2085 described a condition where the root delay was included twice, causing the jitter value to be higher than expected. Due to a misinterpretation of a small-print variable in The Book, the fix for this problem was incorrect, resulting in a root distance that did not include the peer dispersion. The calculations and formulae have been reviewed and reconciled, and the code has been updated accordingly.	ntp	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2340
4879	CVE-2016-7431	MEDIUM	Medium	Zero Origin timestamp problems were fixed by Bug 2945 in ntp-4.2.8p6. However, subsequent timestamp validation checks introduced a regression in the handling of some Zero origin timestamp checks.	ntp	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2336
4880	CVE-2016-7429	MEDIUM	Low	When ntpd receives a server response on a socket that corresponds to a different interface than was used for the request, the peer structure is updated to use the interface for new requests. If ntpd is running on a host with multiple interfaces in separate networks and the operating system doesn't check source address in received packets (e.g. rp_filter on Linux is set to 0), an attacker that knows the address of the source can send a packet with spoofed source address which will cause ntpd to select wrong interface for the source and prevent it from sending new requests until the list of interfaces is refreshed, which happens on routing changes or every 5 minutes by default. If the attack is repeated often enough (once per second), ntpd will not be able to synchronize with the source.	ntp	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2338
4881	CVE-2016-7428	LOW	Medium	The broadcast mode of NTP is expected to only be used in a trusted network. If the broadcast network is accessible to an attacker, a potentially exploitable denial of service vulnerability in ntpd's broadcast mode poll interval enforcement functionality can be abused. To limit abuse, ntpd restricts the rate at which each broadcast association will process incoming packets. ntpd will reject broadcast mode packets that arrive before the poll interval specified in the preceding broadcast packet expires. An attacker with access to the NTP broadcast domain can send specially crafted broadcast mode NTP packets to the broadcast domain which, while being logged by ntpd, will cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers.	ntp	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2334
4882	CVE-2016-7427	LOW	Medium	he broadcast mode of NTP is expected to only be used in a trusted network. If the broadcast network is accessible to an attacker, a potentially exploitable denial of service vulnerability in ntpd's broadcast mode replay prevention functionality can be abused. An attacker with access to the NTP broadcast domain can periodically inject specially crafted broadcast mode NTP packets into the broadcast domain which, while being logged by ntpd, can cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers.	ntp	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2333
4883	CVE-2016-7426	MEDIUM	Medium	When ntpd is configured with rate limiting for all associations (restrict default limited in ntp.conf), the limits are applied also to responses received from its configured sources. An attacker who knows the sources (e.g., from an IPv4 refid in server response) and knows the system is (mis)configured in this way can periodically send packets with spoofed source address to keep the rate limiting activated and prevent ntpd from accepting valid responses from its sources.	ntp	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2339
4884	CVE-2016-7425	HIGH	High	The arcmsr_iop_message_xfer function in drivers/scsi/arcmsr/arcmsr_hba.c in the Linux kernel through 4.8.2 does not restrict a certain length field, which allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) via an ARCMSR_MESSAGE_WRITE_WQBUFFER control code.	linux	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1837
4885	CVE-2016-7424	MEDIUM	Medium	The put_no_rnd_pixels8_xy2_mmx function in x86/rnd_template.c in libav 11.7 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted MP3 file.	libav	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1711
4886	CVE-2016-7423	LOW	Medium	The mptsas_process_scsi_io_request function in QEMU (aka Quick Emulator), when built with LSI SAS1068 Host Bus emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via vectors involving MPTSASRequest objects.	qemu	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1722
4887	CVE-2016-7422	LOW	Medium	The virtqueue_map_desc function in hw/virtio/virtio.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) via a large I/O descriptor buffer length value.	qemu	Unchanged	Not vulnerable	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2801
4888	CVE-2016-7421	LOW	Medium	The pvscsi_ring_pop_req_descr function in hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by leveraging failure to limit process IO loop to the ring size.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2791

	A	B	C	D	E	F	G	H	I	J	K	L	M
4889	CVE-2016-7418	MEDIUM	High	The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service (invalid pointer access and out-of-bounds read) or possibly have unspecified other impact via an incorrect boolean element in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1628
4890	CVE-2016-7417	HIGH	Critical	ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1641
4891	CVE-2016-7416	MEDIUM	High	ext/intl/msgformat/msgformat_format.c in PHP before 5.6.26 and 7.x before 7.0.11 does not properly restrict the locale length provided to the Locale class in the ICU library, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a MessageFormatter::formatMessage call with a long first argument.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1620
4892	CVE-2016-7414	HIGH	Critical	The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to ext/phar/util.c and ext/phar/zip.c.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1635
4893	CVE-2016-7413	HIGH	Critical	Use-after-free vulnerability in the wddx_stack_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to mishandling in a wddx_deserialize call.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1633
4894	CVE-2016-7412	MEDIUM	High	ext/mysqlnd/mysqlnd_wireprotocol.c in PHP before 5.6.26 and 7.x before 7.0.11 does not verify that a BIT field has the UNSIGNED_FLAG flag, which allows remote MySQL servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted field metadata.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1604
4895	CVE-2016-7411	HIGH	Critical	ext/standard/var_unserializer.re in PHP before 5.6.26 mishandles object-deserialization failures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an unserialize call that references a partially constructed object.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1629
4896	CVE-2016-7409	LOW	Medium	dbclient or dropbear server could expose process memory to the running user if compiled with DEBUG_TRACE and running with -v????????????????????????????????	dropbear	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3066
4897	CVE-2016-7408	MEDIUM	High	dbclient could run arbitrary code as the local dbclient user if particular -m or -c arguments are provided. This could be an issue where dbclient is used in scripts.	dropbear	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3065
4898	CVE-2016-7407	HIGH	Critical	dropbearconvert import of OpenSSH keys could run arbitrary code as the local dropbearconvert user when parsing malicious key files	dropbear	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3064
4899	CVE-2016-7406	HIGH	Critical	A dbclient user who can control username or host arguments could potentially run arbitrary code as the dbclient user. This could be a problem if scripts or webpages pass untrusted input to the dbclient program.	dropbear	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3063
4900	CVE-2016-7393	MEDIUM	Medium	Stack-based buffer overflow in the aac_sync function in aac_parser.c in Libav before 11.5 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	libav	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3378
4901	CVE-2016-7180	MEDIUM	Medium	epan/dissectors/packet-ipmi-trace.c in the IPMI trace dissector in Wireshark 2.x before 2.0.6 does not properly consider whether a string is constant, which allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1575
4902	CVE-2016-7179	MEDIUM	Medium	Stack-based buffer overflow in epan/dissectors/packet-catapult-dct2000.c in the Catapult DCT2000 dissector in Wireshark 2.x before 2.0.6 allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1561
4903	CVE-2016-7178	MEDIUM	Medium	epan/dissectors/packet-umts_fp.c in the UMTS FP dissector in Wireshark 2.x before 2.0.6 does not ensure that memory is allocated for certain data structures, which allows remote attackers to cause a denial of service (invalid write access and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1568
4904	CVE-2016-7177	MEDIUM	Medium	epan/dissectors/packet-catapult-dct2000.c in the Catapult DCT2000 dissector in Wireshark 2.x before 2.0.6 does not restrict the number of channels, which allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1557
4905	CVE-2016-7176	MEDIUM	Medium	epan/dissectors/packet-h225.c in the H.225 dissector in Wireshark 2.x before 2.0.6 calls snprintf with one of its input buffers as the output buffer, which allows remote attackers to cause a denial of service (copy overlap and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1565
4906	CVE-2016-7175	MEDIUM	Medium	epan/dissectors/packet-qnet6.c in the QNX6 QNET dissector in Wireshark 2.x before 2.0.6 mishandles MAC address data, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1572
4907	CVE-2016-7170	LOW	Medium	The vmsvga_fifo_run function in hw/display/vmware_vga.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via vectors related to cursor.mask[] and cursor.image[] array sizes when processing a DEFINE_CURSOR svga command.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2783

	A	B	C	D	E	F	G	H	I	J	K	L	M
4908	CVE-2016-7167	HIGH	Critical	It was found that provided string length arguments in four libcurl functions curl_escape(), curl_easy_escape(), curl_unescape and curl_easy_unescape were not properly checked and due to arithmetic in the functions, passing in the length 0xffffffff (2^32-1 or UINT_MAX or even just -1) would end up causing an allocation of zero bytes of heap memory that curl would attempt to write gigabytes of data into.	curl	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1646
4909	CVE-2016-7166	MEDIUM	Medium	libarchive before 3.2.0 does not limit the number of recursive decompressions, which allows remote attackers to cause a denial of service (memory consumption and application crash) via a crafted gzip file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1718
4910	CVE-2016-7164	MEDIUM	High	The construct function in puff.cpp in Libtorrent 1.1.0 allows remote torrent trackers to cause a denial of service (segmentation fault and crash) via a crafted GZIP response.	libtorrent	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3229
4911	CVE-2016-7161	HIGH	Critical	Heap-based buffer overflow in the .receive callback of xlnx.xps-ethernetlite in QEMU (aka Quick Emulator) allows attackers to execute arbitrary code on the QEMU host via a large ethlite packet.	qemu	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1732
4912	CVE-2016-7157	LOW	Medium	The (1) mptsas_config_manufacturing_1 and (2) mptsas_config_ioc_0 functions in hw/scsi/mptconfig.c in QEMU (aka Quick Emulator) allow local guest OS administrators to cause a denial of service (QEMU process crash) via vectors involving MPTSAS_CONFIG_PACK.	qemu	Unchanged	Not vulnerable	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2765
4913	CVE-2016-7156	LOW	Medium	The pvscsi_convert_sglist function in hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by leveraging an incorrect cast.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2729
4914	CVE-2016-7155	LOW	Medium	hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of-bounds access or infinite loop, and QEMU process crash) via a crafted page count for descriptor rings.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2730
4915	CVE-2016-7141	MEDIUM	High	After testing original CVE-2016-5420 patch, it was discovered that libcurl built on top of NSS (Network Security Services) still incorrectly re-uses client certificates if a certificate from file is used for one TLS connection but no certificate is set for a subsequent TLS connection.	curl	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1647
4916	CVE-2016-7134	HIGH	Critical	ext/curl/interface.c in PHP 7.x before 7.0.10 does not work around a libcurl integer overflow, which allows remote attackers to cause a denial of service (allocation error and heap-based buffer overflow) or possibly have unspecified other impact via a long string that is mishandled in a curl_escape call.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1613
4917	CVE-2016-7133	MEDIUM	High	Zend/zend_alloc.c in PHP 7.x before 7.0.10, when open_basedir is enabled, mishandles huge realloc operations, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a long pathname.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1630
4918	CVE-2016-7132	MEDIUM	High	ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a stray element inside a boolean element, leading to incorrect pop processing.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1624
4919	CVE-2016-7131	MEDIUM	High	ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via a malformed wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a tag that lacks a < (less than) character.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1614
4920	CVE-2016-7130	MEDIUM	High	The php_wddx_pop_element function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid base64 binary value, as demonstrated by a wddx_deserialize call that mishandles a binary element in a wddxPacket XML document.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1621
4921	CVE-2016-7129	HIGH	Critical	The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call that mishandles a dateTime element in a wddxPacket XML document.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1608
4922	CVE-2016-7128	MEDIUM	Medium	The exif_process_IFD_in_TIFF function in ext/exif/exif.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1622
4923	CVE-2016-7127	HIGH	Critical	The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1632
4924	CVE-2016-7126	HIGH	Critical	The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which allows remote attackers to cause a denial of service (select_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1627

	A	B	C	D	E	F	G	H	I	J	K	L	M
4925	CVE-2016-7125	MEDIUM	High	ext/session/session.c in PHP before 5.6.25 and 7.x before 7.0.10 skips invalid session names in a way that triggers incorrect parsing, which allows remote attackers to inject arbitrary-type session data by leveraging control of a session name, as demonstrated by object injection.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1610
4926	CVE-2016-7124	HIGH	Critical	ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.	php	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1642
4927	CVE-2016-7122	MEDIUM	Medium	The avi_read_nikon function in libavformat/avidec.c in FFmpeg before 3.1.4 is vulnerable to infinite loop when it decodes an AVI file that has a crafted 'nctg' structure.	gst-ffmpeg	Unchanged	Won't Fix	9.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2880
4928	CVE-2016-7117	HIGH	Critical	Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1729
4929	CVE-2016-7116	LOW	Medium	Directory traversal vulnerability in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to access host files outside the export path via a .. (dot dot) in an unspecified string.	qemu	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2702
4930	CVE-2016-7101	MEDIUM	Medium	The SGI coder in ImageMagick before 7.0.2-10 allows remote attackers to cause a denial of service (out-of-bounds read) via a large row value in an sgi file.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3272
4931	CVE-2016-7098	MEDIUM	High	Race condition in wget 1.17 and earlier, when used in recursive or mirroring mode to download a single file, might allow remote servers to bypass intended access list restrictions by keeping an HTTP connection open.	wget	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1738
4932	CVE-2016-7097	LOW	Medium	The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions.	linux	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1831
4933	CVE-2016-7076	HIGH	HIGH	sudo before version 1.8.18p1 is vulnerable to a bypass in the sudo noexec restriction if application run via sudo executed wordexp() C library function with a user supplied argument. A local user permitted to run such application via sudo with noexec restriction could possibly use this flaw to execute arbitrary commands with elevated privileges.	sudo	Unchanged	8.0.0.27	9.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4047
4934	CVE-2016-7075	MEDIUM	HIGH	It was found that Kubernetes as used by Openshift Enterprise 3 did not correctly validate X.509 client intermediate certificate host name fields. An attacker could use this flaw to bypass authentication requirements by using a specially crafted X.509 certificate.	kubernetes	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4674
4935	CVE-2016-7067	MEDIUM	MEDIUM	The forms in Monit's Service Manager are vulnerable to a cross site request forgery attack.	monit	Unchanged	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3933
4936	CVE-2016-7056	LOW	MEDIUM	The signing function in crypto/ecdsa/ecdsa_ossl.c in certain OpenSSL versions and forks is vulnerable to timing attacks when signing with the standardized elliptic curve P-256 despite featuring constant-time curve operations and modular inversion. A software defect omits setting the BN_FLG_CONSTTIME flag for nonces, failing to take a secure code path in the BN_mod_inverse method and therefore resulting in a cache-timing attack vulnerability. A malicious user with local access can recover ECDSA P-256 private keys.	openssl & libcrypt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3071
4937	CVE-2016-7055	LOW	Medium	There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure that handles input lengths divisible by, but longer than 256 bits. Analysis suggests that attacks against RSA, DSA and DH private keys are impossible. This is because the subroutine in question is not used in operations with the private key itself and an input of the attacker's direct choice. Otherwise the bug can manifest itself as transient authentication and key negotiation failures or reproducible erroneous outcome of public-key operations with specially crafted input. Among EC algorithms only Brainpool P-512 curves are affected and one presumably can attack ECDH key negotiation. Impact was not analyzed in detail, because pre-requisites for attack are considered unlikely. Namely multiple clients have to choose the curve in question and the server has to share the private key among them, neither of which is default behaviour. Even then only clients that chose the curve will be affected.	openssl	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2194
4938	CVE-2016-7054	MEDIUM	High	TLS connections using *-CHACHA20-POLY1305 ciphersuites are susceptible to a DoS attack by corrupting larger payloads. This can result in an OpenSSL crash. This issue is not considered to be exploitable beyond a DoS.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2192
4939	CVE-2016-7053	MEDIUM	High	Applications parsing invalid CMS structures can crash with a NULL pointer dereference. This is caused by a bug in the handling of the ASN.1 CHOICE type in OpenSSL 1.1.0 which can result in a NULL value being passed to the structure callback if an attempt is made to free certain invalid encodings. Only CHOICE structures using a callback which do not handle NULL value are affected.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2193
4940	CVE-2016-7052	MEDIUM	High	crypto/x509/x509_vfy.c in OpenSSL 1.0.2i allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) by triggering a CRL operation.	openssl	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1665
4941	CVE-2016-7048	HIGH	HIGH	The interactive installer in PostgreSQL before 9.3.15, 9.4.x before 9.4.10, and 9.5.x before 9.5.5 might allow remote attackers to execute arbitrary code by leveraging use of HTTP to download software.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4605

	A	B	C	D	E	F	G	H	I	J	K	L	M
4942	CVE-2016-7042	MEDIUM	Medium	The proc_keys_show function in security/keys/proc.c in the Linux kernel through 4.8.2, when the GNU Compiler Collection (gcc) stack protector is enabled, uses an incorrect buffer size for certain timeout data, which allows local users to cause a denial of service (stack memory corruption and panic) by reading the /proc/keys file.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1827
4943	CVE-2016-7039	HIGH	High	The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666.	linux	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1836
4944	CVE-2016-7035	HIGH	HIGH	An authorization flaw was found in Pacemaker before 1.1.16, where it did not properly guard its IPC interface. An attacker with an unprivileged account on a Pacemaker node could use this flaw to, for example, force the Local Resource Manager daemon to execute a script as root and thereby gain root access on the machine.	pacemaker	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4708
4945	CVE-2016-7032	MEDIUM	High	sudo_noexec.so in Sudo before 1.8.15 on Linux might allow local users to bypass intended noexec command restrictions via an application that calls the (1) system or (2) popen function.	sudo	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4053
4946	CVE-2016-6920	MEDIUM	High	Heap-based buffer overflow in the decode_block function in libavcodec/exr.c in FFmpeg before 3.1.3 allows remote attackers to cause a denial of service (application crash) via vectors involving tile positions.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3279
4947	CVE-2016-6912	HIGH	Critical	Double free vulnerability in the gdImageWebPtr function in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified impact via large width and height values.	libgd	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3312
4948	CVE-2016-6911	MEDIUM	Medium	The dynamicGetbuf function in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TIFF image.	libgd	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3167
4949	CVE-2016-6906	MEDIUM	Medium	The read_image_tga function in gd_tga.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file, related to the decompression buffer.	gd	Unchanged	8.0.0.18	9.0.0.7	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3651
4950	CVE-2016-6905	MEDIUM	Medium	The read_image_tga function in gd_tga.c in the GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA image.	gd	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1727
4951	CVE-2016-6888	LOW	Medium	Integer overflow in the net_tx_pkt_init function in hw/net/net_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (QEMU process crash) via the maximum fragmentation count, which triggers an unchecked multiplication and NULL pointer dereference.	qemu	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2781
4952	CVE-2016-6881	MEDIUM	Medium	The zlib_refill function in libavformat/swfdec.c in FFmpeg before 3.1.3 allows remote attackers to cause an infinite loop denial of service via a crafted SWF file.	gst-ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2878
4953	CVE-2016-6836	LOW	Medium	The vmxnet3_complete_packet function in hw/net/vmxnet3.c in QEMU (aka Quick Emulator) allows local guest OS administrators to obtain sensitive host memory information by leveraging failure to initialize the txcq_descr object.	qemu	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2704
4954	CVE-2016-6835	LOW	Medium	The vmxnet_tx_pkt_parse_headers function in hw/net/vmxnet_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (buffer over-read) by leveraging failure to check IP header length.	qemu	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2727
4955	CVE-2016-6834	LOW	Medium	The net_tx_pkt_do_sw_fragmentation function in hw/net/net_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via a zero length for the current fragment length.	qemu	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2787
4956	CVE-2016-6833	LOW	Medium	Use-after-free vulnerability in the vmxnet3_io_bar0_write function in hw/net/vmxnet3.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (QEMU instance crash) by leveraging failure to check if the device is active.	qemu	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2795
4957	CVE-2016-6832	MEDIUM	Medium	Heap-based buffer overflow in the ff_audio_resample function in resample.c in libav before 11.4 allows remote attackers to cause a denial of service (crash) via vectors related to buffer resizing.	libav	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3394
4958	CVE-2016-6828	MEDIUM	Medium	The tcp_check_send_head function in include/net/tcp.h in the Linux kernel before 4.7.5 does not properly maintain certain SACK state after a failed data copy, which allows local users to cause a denial of service (tcp_xmit_retransmit_queue use-after-free and system crash) via a crafted SACK option.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1826
4959	CVE-2016-6823	MEDIUM	High	Integer overflow in the BMP coder in ImageMagick before 7.0.2-10 allows remote attackers to cause a denial of service (crash) via crafted height and width values, which triggers an out-of-bounds write.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3205
4960	CVE-2016-6787	MEDIUM	High	kernel/events/core.c in the performance subsystem in the Linux kernel before 4.0 mismanages locks during certain migrations, which allows local users to gain privileges via a crafted application, aka Android internal bug 31095224.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2856
4961	CVE-2016-6786	MEDIUM	High	kernel/events/core.c in the performance subsystem in the Linux kernel before 4.0 mismanages locks during certain migrations, which allows local users to gain privileges via a crafted application, aka Android internal bug 30955111.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2884

	A	B	C	D	E	F	G	H	I	J	K	L	M
4962	CVE-2016-6711	HIGH	Medium	A remote denial of service vulnerability in libvpx in Mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-11-01 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-30593765.	libvpx	Unchanged	8.0.0.13	9.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2728
4963	CVE-2016-6671	MEDIUM	High	The raw_decode function in libavcodec/rawdec.c in FFmpeg before 3.1.2 allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted SWF file.	gst-ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2863
4964	CVE-2016-6664	MEDIUM	High	mysqld_safe in Oracle MySQL through 5.5.51, 5.6.x through 5.6.32, and 5.7.x through 5.7.14; MariaDB; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17, when using file-based logging, allows local users with access to the mysql account to gain root privileges via a symlink attack on error logs and possibly other files.	mysql	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2688
4965	CVE-2016-6663	MEDIUM	High	Race condition in Oracle MySQL before 5.5.52, 5.6.x before 5.6.33, 5.7.x before 5.7.15, and 8.x before 8.0.1; MariaDB before 5.5.52 and 10.1.x before 10.1.18; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17 allows local users with certain permissions to gain privileges by leveraging use of my_copystat by REPAIR TABLE to repair a MyISAM table.	mysql	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2677
4966	CVE-2016-6662	HIGH	High	Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib.	mysql	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1605
4967	CVE-2016-6633	MEDIUM	High	An issue was discovered in phpMyAdmin. phpMyAdmin can be used to trigger a remote code execution attack against certain PHP installations that are running with the dbase extension. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2800
4968	CVE-2016-6632	MEDIUM	Medium	An issue was discovered in phpMyAdmin where, under certain conditions, phpMyAdmin may not delete temporary files during the import of ESRI files. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2698
4969	CVE-2016-6631	HIGH	High	An issue was discovered in phpMyAdmin. A user can execute a remote code execution attack against a server when phpMyAdmin is being run as a CGI application. Under certain server configurations, a user can pass a query string which is executed as a command-line argument by the file generator_plugin.sh. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2770
4970	CVE-2016-6630	MEDIUM	Medium	An issue was discovered in phpMyAdmin. An authenticated user can trigger a denial-of-service (DoS) attack by entering a very long password at the change password dialog. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2676
4971	CVE-2016-6629	HIGH	Critical	An issue was discovered in phpMyAdmin involving the $cfg['ArbitraryServerRegexp'] configuration directive. An attacker could reuse certain cookie values in a way of bypassing the servers defined by ArbitraryServerRegexp. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2784
4972	CVE-2016-6628	MEDIUM	Medium	An issue was discovered in phpMyAdmin. An attacker may be able to trigger a user to download a specially crafted malicious SVG file. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2699
4973	CVE-2016-6627	MEDIUM	Medium	An issue was discovered in phpMyAdmin. An attacker can determine the phpMyAdmin host location through the file url.php. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2793
4974	CVE-2016-6626	MEDIUM	Medium	An issue was discovered in phpMyAdmin. An attacker could redirect a user to a malicious web page. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2776
4975	CVE-2016-6625	MEDIUM	Medium	An issue was discovered in phpMyAdmin. An attacker can determine whether a user is logged in to phpMyAdmin. The user's session, username, and password are not compromised by this vulnerability. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2768

	A	B	C	D	E	F	G	H	I	J	K	L	M
4976	CVE-2016-6624	MEDIUM	Medium	An issue was discovered in phpMyAdmin involving improper enforcement of the IP-based authentication rules. When phpMyAdmin is used with IPv6 in a proxy server environment, and the proxy server is in the allowed range but the attacking computer is not allowed, this vulnerability can allow the attacking computer to connect despite the IP rules. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2693
4977	CVE-2016-6623	MEDIUM	Medium	An issue was discovered in phpMyAdmin. An authorized user can cause a denial-of-service (DoS) attack on a server by passing large values to a loop. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2777
4978	CVE-2016-6622	MEDIUM	Medium	An issue was discovered in phpMyAdmin. An unauthenticated user is able to execute a denial-of-service (DoS) attack by forcing persistent connections when phpMyAdmin is running with $cfg['AllowArbitraryServer']=true. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2799
4979	CVE-2016-6621	MEDIUM	High	The setup script for phpMyAdmin before 4.0.10.19, 4.4.x before 4.4.15.10, and 4.6.x before 4.6.6 allows remote attackers to conduct server-side request forgery (SSRF) attacks via unspecified vectors.	phpMyAdmin	Unchanged	8.0.0.16	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3308
4980	CVE-2016-6620	HIGH	Critical	An issue was discovered in phpMyAdmin. Some data is passed to the PHP unserialize() function without verification that it's valid serialized data. The unserialization can result in code execution because of the interaction with object instantiation and autoloading. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2764
4981	CVE-2016-6619	MEDIUM	High	An issue was discovered in phpMyAdmin. In the user interface preference feature, a user can execute an SQL injection attack against the account of the control user. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2771
4982	CVE-2016-6618	MEDIUM	Medium	An issue was discovered in phpMyAdmin. The transformation feature allows a user to trigger a denial-of-service (DoS) attack against the server. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2789
4983	CVE-2016-6617	MEDIUM	High	An issue was discovered in phpMyAdmin. A specially crafted database and/or table name can be used to trigger an SQL injection attack through the export functionality. All 4.6.x versions (prior to 4.6.4) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2664
4984	CVE-2016-6616	MEDIUM	High	An issue was discovered in phpMyAdmin. In the User group and Designer features, a user can execute an SQL injection attack against the account of the control user. All 4.6.x versions (prior to 4.6.4) and 4.4.x versions (prior to 4.4.15.8) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2753
4985	CVE-2016-6615	MEDIUM	Medium	XSS issues were discovered in phpMyAdmin. This affects navigation pane and database/table hiding feature (a specially-crafted database name can be used to trigger an XSS attack); the Tracking feature (a specially-crafted query can be used to trigger an XSS attack); and GIS visualization feature. All 4.6.x versions (prior to 4.6.4) and 4.4.x versions (prior to 4.4.15.8) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2745
4986	CVE-2016-6614	MEDIUM	Medium	An issue was discovered in phpMyAdmin involving the %u username replacement functionality of the SaveDir and UploadDir features. When the username substitution is configured, a specially-crafted user name can be used to circumvent restrictions to traverse the file system. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2696
4987	CVE-2016-6613	LOW	Medium	An issue was discovered in phpMyAdmin. A user can specially craft a symlink on disk, to a file which phpMyAdmin is permitted to read but the user is not, which phpMyAdmin will then expose to the user. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2751
4988	CVE-2016-6612	MEDIUM	Medium	An issue was discovered in phpMyAdmin. A user can exploit the LOAD LOCAL INFILE functionality to expose files on the server to the database system. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2762
4989	CVE-2016-6611	MEDIUM	High	An issue was discovered in phpMyAdmin. A specially crafted database and/or table name can be used to trigger an SQL injection attack through the export functionality. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2761
4990	CVE-2016-6610	MEDIUM	Medium	A full path disclosure vulnerability was discovered in phpMyAdmin where a user can trigger a particular error in the export mechanism to discover the full path of phpMyAdmin on the disk. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2720
4991	CVE-2016-6609	MEDIUM	High	An issue was discovered in phpMyAdmin. A specially crafted database name could be used to run arbitrary PHP commands through the array export feature. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2707

	A	B	C	D	E	F	G	H	I	J	K	L	M
4992	CVE-2016-6608	MEDIUM	Medium	XSS issues were discovered in phpMyAdmin. This affects the database privilege check and the Remove partitioning functionality. Specially crafted database names can trigger the XSS attack. All 4.6.x versions (prior to 4.6.4) are affected.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2679
4993	CVE-2016-6607	MEDIUM	Medium	XSS issues were discovered in phpMyAdmin. This affects Zoom search (specially crafted column content can be used to trigger an XSS attack); GIS editor (certain fields in the graphical GIS editor are not properly escaped and can be used to trigger an XSS attack); Relation view; the following Transformations: Formatted, Imagelink, JPEG: Upload, RegexValidation, JPEG inline, PNG inline, and transformation wrapper; XML export; MediaWiki export; Designer; When the MySQL server is running with a specially-crafted log_bin directive; Database tab; Replication feature; and Database search. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2792
4994	CVE-2016-6606	MEDIUM	High	An issue was discovered in cookie encryption in phpMyAdmin. The decryption of the username/password is vulnerable to a padding oracle attack. This can allow an attacker who has access to a user's browser cookie file to decrypt the username and password. Furthermore, the same initialization vector (IV) is used to hash the username and password stored in the phpMyAdmin cookie. If a user has the same password as their username, an attacker who examines the browser cookie can see that they are the same - but the attacker can not directly decode these values from the cookie as it is still hashed. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected.	phpmyadmin	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2759
4995	CVE-2016-6520	MEDIUM	Critical	Buffer overflow in MagickCore/enhance.c in ImageMagick before 7.0.2-7 allows remote attackers to have unspecified impact via vectors related to pixel cache morphology.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2774
4996	CVE-2016-6516	MEDIUM	High	Race condition in the ioctl_file_dedupe_range function in fs/ioctl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (heap-based buffer overflow) or possibly gain privileges by changing a certain count value, aka a double fetch vulnerability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1364
4997	CVE-2016-6515	HIGH	High	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.	openssh	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1435
4998	CVE-2016-6513	MEDIUM	Medium	epan/dissectors/packet-wbxml.c in the WBXML dissector in Wireshark 2.x before 2.0.5 does not restrict the recursion depth, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1410
4999	CVE-2016-6512	MEDIUM	Medium	epan/dissectors/packet-wap.c in Wireshark 2.x before 2.0.5 omits an overflow check in the tvb_get_guintvar function, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet, related to the MMSE, WAP, WBXML, and WSP dissectors.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1430
5000	CVE-2016-6511	MEDIUM	Medium	epan/proto.c in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 allows remote attackers to cause a denial of service (OpenFlow dissector large loop) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1378
5001	CVE-2016-6510	MEDIUM	Medium	Off-by-one error in epan/dissectors/packet-rlc.c in the RLC dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1402
5002	CVE-2016-6509	MEDIUM	Medium	epan/dissectors/packet-ldss.c in the LDSS dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 mishandles conversations, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1367
5003	CVE-2016-6508	MEDIUM	Medium	epan/dissectors/packet-rlc.c in the RLC dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 uses an incorrect integer data type, which allows remote attackers to cause a denial of service (large loop) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1415
5004	CVE-2016-6507	MEDIUM	Medium	epan/dissectors/packet-mmse.c in the MMSE dissector in Wireshark 1.12.x before 1.12.13 allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1385
5005	CVE-2016-6506	MEDIUM	Medium	epan/dissectors/packet-wsp.c in the WSP dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1427
5006	CVE-2016-6505	MEDIUM	Medium	epan/dissectors/packet-packetbb.c in the PacketBB dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1406
5007	CVE-2016-6504	MEDIUM	Medium	epan/dissectors/packet-ncp2222.inc in the NDS dissector in Wireshark 1.12.x before 1.12.13 does not properly maintain a ptvc data structure, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1375
5008	CVE-2016-6503	MEDIUM	Medium	The CORBA IDL dissectors in Wireshark 2.x before 2.0.5 on 64-bit Windows platforms do not properly interact with Visual C++ compiler options, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1420

	A	B	C	D	E	F	G	H	I	J	K	L	M
5009	CVE-2016-6491	MEDIUM	High	Buffer overflow in the Get8BIMProperty function in MagickCore/property.c in ImageMagick before 6.9.5-4 and 7.x before 7.0.2-6 allows remote attackers to cause a denial of service (out-of-bounds read, memory leak, and crash) via a crafted image.	imagemagick	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2794
5010	CVE-2016-6490	LOW	Medium	The virtqueue_map_desc function in hw/virtio/virtio.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via a zero length for the descriptor buffer.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2748
5011	CVE-2016-6480	MEDIUM	Medium	Race condition in the ioctl_send_fib function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (out-of-bounds access or system crash) by changing a certain size value, aka a double fetch vulnerability.	linux	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1400
5012	CVE-2016-6354	HIGH	Critical	Heap-based buffer overflow in the yy_get_next_buffer function in Flex before 2.6.1 might allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code via vectors involving num_to_read.	flex	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1712
5013	CVE-2016-6352	MEDIUM	High	The OneLine32 function in io-ico.c in gdk-pixbuf before 2.35.3 allows remote attackers to cause a denial of service (out-of-bounds write and crash) via crafted dimensions in an ICO file.	gdk-pixbuf	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1719
5014	CVE-2016-6351	HIGH	High	The esp_do_dma function in hw/scsi/esp.c in QEMU (aka Quick Emulator), when built with ESP/NCR53C9x controller emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) or execute arbitrary code on the QEMU host via vectors involving DMA read into ESP command buffer.	qemu	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1573
5015	CVE-2016-6329	MEDIUM	Medium	OpenVPN, when using a 64-bit block cipher, makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTP-over-OpenVPN session using Blowfish in CBC mode, aka a Sweet32 attack.	openvpn	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3192
5016	CVE-2016-6327	MEDIUM	Medium	drivers/infiniband/ulp/srpt/ib_srpt.c in the Linux kernel before 4.5.1 allows local users to cause a denial of service (NULL pointer dereference and system crash) by using an ABORT_TASK command to abort a device write operation.	linux	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1830
5017	CVE-2016-6323	MEDIUM	High	The makecontext function in the GNU C Library (aka glibc or libc6) before 2.25 creates execution contexts incompatible with the unwinder on ARM EABI (32-bit) platforms, which might allow context-dependent attackers to cause a denial of service (hang), as demonstrated by applications compiled using gccgo, related to backtrace generation.	glibc	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1747
5018	CVE-2016-6321	MEDIUM	High	Directory traversal vulnerability in the safer_name_suffix function in GNU tar 1.14 through 1.29 might allow remote attackers to bypass an intended protection mechanism and write to arbitrary files via vectors related to improper sanitization of the file_name parameter, aka POINTYFEATHER.	tar	Unchanged	8.0.0.13	9.0.0.4	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2734
5019	CVE-2016-6318	HIGH	High	Stack-based buffer overflow in the FascistGecosUser function in lib/fascist.c in cracklib allows local users to cause a denial of service (application crash) or gain privileges via a long GECOS field, involving longbuffer.	cracklib	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1563
5020	CVE-2016-6313	MEDIUM	Medium	The mixing functions in the random number generator in Libgcrypt before 1.5.6, 1.6.x before 1.6.6, and 1.7.x before 1.7.3 and GnuPG before 1.4.21 make it easier for attackers to obtain the values of 160 bits by leveraging knowledge of the previous 4640 bits.	libgcrypt	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2775
5021	CVE-2016-6312	MEDIUM	Medium	The mod_dontdothat component of the mod_dav_svn Apache module in Subversion as packaged in Red Hat Enterprise Linux 5.11 does not properly detect recursion during entity expansion, which allows remote authenticated users with access to the webdav repository to cause a denial of service (memory consumption and httpd crash). NOTE: Exists as a regression to CVE-2009-1955.	subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4845
5022	CVE-2016-6309	HIGH	Critical	statem/statem.c in OpenSSL 1.1.0a does not consider memory-block movement after a realloc call, which allows remote attackers to cause a denial of service (use-after-free) or possibly execute arbitrary code via a crafted TLS session.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1664
5023	CVE-2016-6308	HIGH	Medium	This issue is very similar to CVE-2016-6307. The underlying defect is different but the security analysis and impacts are the same except that it impacts DTLS.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1645
5024	CVE-2016-6307	MEDIUM	Medium	A TLS message includes 3 bytes for its length in the header for the message. This would allow for messages up to 16Mb in length. Messages of this length are excessive and OpenSSL includes a check to ensure that a peer is sending reasonably sized messages in order to avoid too much memory being consumed to service a connection. A flaw in the logic of version 1.1.0 means that memory for the message is allocated too early, prior to the excessive message length check. Due to way memory is allocated in OpenSSL this could mean an attacker could force up to 21Mb to be allocated to service a connection. This could lead to a Denial of Service through memory exhaustion. However, the excessive message length check still takes place, and this would cause the connection to immediately fail. Assuming that the application calls SSL_free() on the failed conneciton in a timely manner then the 21Mb of allocated memory will then be immediately freed again. Therefore the excessive memory allocation will be transitory in nature. This then means that there is only a security impact if	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1644

	A	B	C	D	E	F	G	H	I	J	K	L	M
5025	CVE-2016-6306	MEDIUM	Medium	In ssl3_get_client_certificate, ssl3_get_server_certificate and ssl3_get_certificate_request check we have enough room before reading a length.	openssl	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1601
5026	CVE-2016-6305	MEDIUM	High	OpenSSL 1.1.0 SSL/TLS will hang during a call to SSL_peek() if the peer sends an empty record. This could be exploited by a malicious peer in a Denial Of Service attack.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1643
5027	CVE-2016-6304	HIGH	High	A memory leak flaw was found in the way OpenSSL handled TLS status request extension data during session renegotiation. A remote attacker could cause a TLS server using OpenSSL to consume an excessive amount of memory and, possibly, exit unexpectedly after exhausting all available memory, if it enabled OCSP stapling support.	openssl	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1603
5028	CVE-2016-6303	HIGH	Critical	Possible integer overflow vulnerability was found in MDC2_Update() function that can lead to out-of-bounds write.	openssl	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1524
5029	CVE-2016-6302	MEDIUM	High	It was found that if a ticket callback changes the HMAC digest to SHA512 the existing sanity checks are not sufficient and an attacker could perform a DoS attack with a malformed ticket.	openssl	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1526
5030	CVE-2016-6301	HIGH	High	The recv_and_process_client_pkt function in networking/ntpd.c in busybox allows remote attackers to cause a denial of service (CPU and bandwidth consumption) via a forged NTP packet, which triggers a communication loop.	busybox	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2687
5031	CVE-2016-6297	MEDIUM	High	Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1281
5032	CVE-2016-6295	HIGH	Critical	ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1300
5033	CVE-2016-6294	HIGH	Critical	The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1306
5034	CVE-2016-6292	MEDIUM	Medium	The exif_process_user_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1288
5035	CVE-2016-6291	HIGH	Critical	The exif_process_IFD_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1289
5036	CVE-2016-6290	HIGH	Critical	ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1268
5037	CVE-2016-6289	MEDIUM	High	Integer overflow in the virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1271
5038	CVE-2016-6288	HIGH	Critical	The php_url_parse_ex function in ext/standard/url.c in PHP before 5.5.38 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via vectors involving the smart_str data type.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1270
5039	CVE-2016-6263	MEDIUM	High	The stringprep_utf8_nfkc_normalize function in lib/nfkc.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted UTF-8 data.	libidn	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1567
5040	CVE-2016-6262	MEDIUM	High	idn in libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read, a different vulnerability than CVE-2015-8948.	libidn	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1566
5041	CVE-2016-6261	MEDIUM	High	The idna_to_ascii_4i function in lib/idna.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via 64 bytes of input.	libidn	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1558
5042	CVE-2016-6255	MEDIUM	High	Portable UPnP SDK (aka libupnp) before 1.6.21 allows remote attackers to write to arbitrary files in the webroot via a POST request without a registered handler.	libupnp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3542
5043	CVE-2016-6254	MEDIUM	Critical	Heap-based buffer overflow in the parse_packet function in network.c in collectd before 5.4.3 and 5.x before 5.5.2 allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted network packet.	collectd	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1506
5044	CVE-2016-6252	MEDIUM	High	Integer overflow in shadow 4.2.1 allows local users to gain privileges via crafted input to newuidmap.	shadow	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4567

	A	B	C	D	E	F	G	H	I	J	K	L	M
5045	CVE-2016-6250	HIGH	High	Integer overflow in the ISO9660 writer in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via vectors related to verifying filename lengths when writing an ISO9660 archive, which trigger a buffer overflow.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1742
5046	CVE-2016-6224	LOW	Low	ecryptfs-setup-swap in eCryptfs does not prevent the unencrypted swap partition from activating during boot when using GPT partitioning on a (1) NVMe or (2) MMC drive, which allows local users to obtain sensitive information via unspecified vectors. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8946.	ecryptfs-utils	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1301
5047	CVE-2016-6223	MEDIUM	Critical	The TIFFReadRawStrip1 and TIFFReadRawTile1 functions in tif_read.c in libtiff before 4.0.7 allows remote attackers to cause a denial of service (crash) or possibly obtain sensitive information via a negative index in a file-content buffer.	libtiff	Unchanged	8.0.0.15	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3163
5048	CVE-2016-6214	MEDIUM	Medium	gd_tga.c in the GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file.	gd	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1416
5049	CVE-2016-6213	MEDIUM	Medium	fs/namespace.c in the Linux kernel before 4.9 does not restrict how many mounts may exist in a mount namespace, which allows local users to cause a denial of service (memory consumption and deadlock) via MS_BIND mount system calls, as demonstrated by a loop that triggers exponential growth in the number of mounts.	linux	Unchanged	8.0.0.13	9.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2864
5050	CVE-2016-6210	MEDIUM	Medium	When SSHD tries to authenticate a non-existing user, it will pick up a fake password structure hardcoded in the SSHD source code. On this hard coded password structure the password hash is based on BLOWFISH ($2) algorithm. If real users passwords are hashed using SHA256/SHA512, then sending large passwords (10KB) will result in shorter response time from the server for non-existing users. This allows remote attacker to enumerate existing users on system logging via SSHD.	openssh	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1662
5051	CVE-2016-6207	MEDIUM	Medium	Integer overflow in the _gdContributionsAlloc function in gd_interpolation.c in GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds memory write or memory consumption) via unspecified vectors.	gd	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1380
5052	CVE-2016-6198	MEDIUM	Medium	The filesystem layer in the Linux kernel before 4.5.5 proceeds with post-rename operations after an OverlayFS file is renamed to a self-hardlink, which allows local users to cause a denial of service (system crash) via a rename system call, related to fs/namei.c and fs/open.c.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1392
5053	CVE-2016-6197	MEDIUM	Medium	fs/overlayfs/dir.c in the OverlayFS filesystem implementation in the Linux kernel before 4.6 does not properly verify the upper dentry before proceeding with unlink and rename system-call processing, which allows local users to cause a denial of service (system crash) via a rename system call that specifies a self-hardlink.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1419
5054	CVE-2016-6187	HIGH	High	The apparmor_setprocattr function in security/apparmor/lsm.c in the Linux kernel before 4.6.5 does not validate the buffer size, which allows local users to gain privileges by triggering an AppArmor setprocattr hook.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1395
5055	CVE-2016-6185	MEDIUM	High	The XSLoader::load method in XSLoader in Perl does not properly locate .so files when called in a string eval, which might allow local users to execute arbitrary code via a Trojan horse library under the current working directory.	perl	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1409
5056	CVE-2016-6170	MEDIUM	Medium	ISC BIND through 9.9.9-P1, 9.10.x through 9.10.4-P1, and 9.11.x through 9.11.0b1 allows primary DNS servers to cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated users to cause a denial of service (primary DNS server crash) via a large UPDATE message.	bind	Unchanged	8.0.0.26	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1125
5057	CVE-2016-6164	HIGH	Critical	Integer overflow in the mov_build_index function in libavformat/mov.c in FFmpeg before 2.8.8, 3.0.x before 3.0.3 and 3.1.x before 3.1.1 allows remote attackers to have unspecified impact via vectors involving sample size.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3174
5058	CVE-2016-6163	MEDIUM	Medium	The rsvg_pattern_fix_fallback function in rsvg-paint_server.c in librsvg2 2.40.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted svg file.	librsvg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3248
5059	CVE-2016-6162	MEDIUM	High	net/core/skbuff.c in the Linux kernel 4.7-rc6 allows local users to cause a denial of service (panic) or possibly have unspecified other impact via certain IPv6 socket operations.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1429
5060	CVE-2016-6161	MEDIUM	Medium	The output function in gd_gif_out.c in the GD Graphics Library (aka libgd) allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image.	gd	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1436
5061	CVE-2016-6160	MEDIUM	High	tcprewrite in tcpreplay before 4.1.2 allows remote attackers to cause a denial of service (segmentation fault) via a large frame.	tcpreplay	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3210
5062	CVE-2016-6156	LOW	Medium	Race condition in the ec_device_ioctl_xcmd function in drivers/platform/chrome/cros_ec_dev.c in the Linux kernel before 4.7 allows local users to cause a denial of service (out-of-bounds array access) by changing a certain size value, aka a double fetch vulnerability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1368
5063	CVE-2016-6153	MEDIUM	Medium	os_unix.c in SQLite before 3.13.0 improperly implements the temporary directory search algorithm, which might allow local users to obtain sensitive information, cause a denial of service (application crash), or have unspecified other impact by leveraging use of the current working directory for temporary files.	sqlite	Unchanged	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1740

	A	B	C	D	E	F	G	H	I	J	K	L	M
5064	CVE-2016-6136	LOW	Medium	Race condition in the audit_log_single_execve_arg function in kernel/auditsc.c in the Linux kernel through 4.7 allows local users to bypass intended character-set restrictions or disrupt system-call auditing by changing a certain string, aka a double fetch vulnerability.	linux	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1407
5065	CVE-2016-6132	MEDIUM	Medium	The gdImageCreateFromTgaCtx function in the GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file.	gd	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1417
5066	CVE-2016-6131	MEDIUM	High	The demangler in GNU Libiberty allows remote attackers to cause a denial of service (infinite loop, stack overflow, and crash) via a cycle in the references of remembered mangled types.	gcc	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3267
5067	CVE-2016-6130	LOW	Medium	Race condition in the sclp_ctl_ioctl_sccb function in drivers/s390/char/sclp_ctl.c in the Linux kernel before 4.6 allows local users to obtain sensitive information from kernel memory by changing a certain length value, aka a double fetch vulnerability.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1122
5068	CVE-2016-6128	MEDIUM	High	The gdImageCropThreshold function in gd_crop.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 7.0.9, allows remote attackers to cause a denial of service (application crash) via an invalid color index.	gd	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1397
5069	CVE-2016-5875			An exploitable heap based buffer overflow exists in the handling of compressed TIFF images in LibTIFF's PixarLogDecode api. A crafted TIFF document can lead to a heap based buffer overflow resulting in remote code execution. The vulnerability can be triggered through any user controlled TIFF that is handled by this functionality.	libtiff	Updated	8.0.0.15	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3450
5070	CVE-2016-5870	MEDIUM	High	The msm_ipc_router_close function in net/ipc_router/ipc_router_socket.c in the ipc_router component for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact by triggering failure of an accept system call for an AF_MSM_IPC socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3952
5071	CVE-2016-5844	MEDIUM	Medium	Integer overflow in the ISO parser in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) via a crafted ISO file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1744
5072	CVE-2016-5842	MEDIUM	High	MagickCore/property.c in ImageMagick before 7.0.2-1 allows remote attackers to obtain sensitive memory information via vectors involving the q variable, which triggers an out-of-bounds read.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2665
5073	CVE-2016-5841	HIGH	Critical	Integer overflow in MagickCore/profile.c in ImageMagick before 7.0.2-1 allows remote attackers to cause a denial of service (segmentation fault) or possibly execute arbitrary code via vectors involving the offset variable.	imagemagick	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2758
5074	CVE-2016-5829	HIGH	High	Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGES or (2) HIDIOCSUSAGES ioctl call.	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-923
5075	CVE-2016-5828	HIGH	High	The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc platforms mishandles transactional state, which allows local users to cause a denial of service (invalid process state or TM Bad Thing exception, and system crash) or possibly have unspecified other impact by starting and suspending a transaction before an exec system call.	linux	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-938
5076	CVE-2016-5827	MEDIUM	High	The icaltime_from_string function in libical 0.47 and 1.0 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted string to the icalparser_parse_string function.	libical	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3155
5077	CVE-2016-5826	MEDIUM	High	The parser_get_next_char function in libical 0.47 and 1.0 allows remote attackers to cause a denial of service (out-of-bounds heap read) by crafting a string to the icalparser_parse_string function.	libical	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3224
5078	CVE-2016-5825	MEDIUM	Medium	The icalparser_parse_string function in libical 0.47 and 1.0 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted ics file.	libical	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3243
5079	CVE-2016-5824	MEDIUM	Medium	libical 1.0 allows remote attackers to cause a denial of service (use-after-free) via a crafted ics file.	libical	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3214
5080	CVE-2016-5823	MEDIUM	Medium	The icalproperty_new_clone function in libical 0.47 and 1.0 allows remote attackers to cause a denial of service (use-after-free) via a crafted ics file.	libical	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3234
5081	CVE-2016-5773	HIGH	Critical	php_zip.c in the zip extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data containing a ZipArchive object.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1376
5082	CVE-2016-5772	HIGH	Critical	Double free vulnerability in the php_wddx_process_data function in wddx.c in the WDDX extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted XML data that is mishandled in a wddx_deserialize call.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1405
5083	CVE-2016-5771	HIGH	Critical	spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1391

	A	B	C	D	E	F	G	H	I	J	K	L	M
5084	CVE-2016-5770	HIGH	Critical	Integer overflow in the SplFileObject::fread function in spl_directory.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer argument, a related issue to CVE-2016-5096.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1389
5085	CVE-2016-5769	HIGH	Critical	Multiple integer overflows in mcrypt.c in the mcrypt extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted length value, related to the (1) mcrypt_generic and (2) mdecrypt_generic functions.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1386
5086	CVE-2016-5768	HIGH	Critical	Double free vulnerability in the _php_mb_regex_ereg_replace_exec function in php_mbregex.c in the mbstring extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by leveraging a callback exception.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1431
5087	CVE-2016-5767	MEDIUM	High	Integer overflow in the gdImageCreate function in gd.c in the GD Graphics Library (aka libgd) before 2.0.34RC1, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted image dimensions.	gd	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1369
5088	CVE-2016-5766	MEDIUM	High	Integer overflow in the _gd2GetHeader function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via crafted chunk dimensions in an image.	gd	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1422
5089	CVE-2016-5739	MEDIUM	High	The Transformation implementation in phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 does not use the no-referrer Content Security Policy (CSP) protection mechanism, which makes it easier for remote attackers to conduct CSRF attacks by reading an authentication token in a Referer header, related to libraries/Header.php.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1124
5090	CVE-2016-5734	HIGH	Critical	phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 does not properly choose delimiters to prevent use of the preg_replace e (aka eval) modifier, which might allow remote attackers to execute arbitrary PHP code via a crafted string, as demonstrated by the table search-and-replace implementation.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1130
5091	CVE-2016-5733	MEDIUM	Medium	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) a crafted table name that is mishandled during privilege checking in table_row.phtml, (2) a crafted mysqld log_bin directive that is mishandled in log_selector.phtml, (3) the Transformation implementation, (4) AJAX error handling in js/ajax.js, (5) the Designer implementation, (6) the charts implementation in js/tbl_chart.js, or (7) the zoom-search implementation in rows_zoom.phtml.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1119
5092	CVE-2016-5732	MEDIUM	Medium	Multiple cross-site scripting (XSS) vulnerabilities in the partition-range implementation in templates/table/structure/display_partitions.phtml in the table-structure page in phpMyAdmin 4.6.x before 4.6.3 allow remote attackers to inject arbitrary web script or HTML via crafted table parameters.	phpmyadmin	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1121
5093	CVE-2016-5731	MEDIUM	Medium	Cross-site scripting (XSS) vulnerability in examples/openid.php in phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 allows remote attackers to inject arbitrary web script or HTML via vectors involving an OpenID error message.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1109
5094	CVE-2016-5730	MEDIUM	Medium	phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 allows remote attackers to obtain sensitive information via vectors involving (1) an array value to FormDisplay.php, (2) incorrect data to validate.php, (3) unexpected data to Validator.php, (4) a missing config directory during setup, or (5) an incorrect OpenID identifier data type, which reveals the full path in an error message.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1117
5095	CVE-2016-5728	MEDIUM	Medium	Race condition in the vop_ioctl function in drivers/misc/mic/vop/vop_vringh.c in the MIC VOP driver in the Linux kernel before 4.6.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (memory corruption and system crash) by changing a certain header, aka a double fetch vulnerability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-934
5096	CVE-2016-5706	MEDIUM	High	js/get_scripts.js.php in phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 allows remote attackers to cause a denial of service via a large array in the scripts parameter.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1129
5097	CVE-2016-5705	MEDIUM	Medium	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.4.x before 4.4.15.7 and 4.6.x before 4.6.3 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) server-privileges certificate data fields on the user privileges page, (2) an invalid JSON error message in the error console, (3) a database name in the central columns implementation, (4) a group name, or (5) a search name in the bookmarks implementation.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1111

	A	B	C	D	E	F	G	H	I	J	K	L	M
5098	CVE-2016-5704	MEDIUM	Medium	Cross-site scripting (XSS) vulnerability in the table-structure page in phpMyAdmin 4.6.x before 4.6.3 allows remote attackers to inject arbitrary web script or HTML via vectors involving a comment.	phpmyadmin	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1118
5099	CVE-2016-5703	HIGH	Critical	SQL injection vulnerability in libraries/central_columns.lib.php in phpMyAdmin 4.4.x before 4.4.15.7 and 4.6.x before 4.6.3 allows remote attackers to execute arbitrary SQL commands via a crafted database name that is mishandled in a central column query.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1127
5100	CVE-2016-5702	MEDIUM	Low	phpMyAdmin 4.6.x before 4.6.3, when the environment lacks a PHP_SELF value, allows remote attackers to conduct cookie-attribute injection attacks via a crafted URI.	phpmyadmin	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1116
5101	CVE-2016-5701	MEDIUM	Medium	setup/frames/index.inc.php in phpMyAdmin 4.0.10.x before 4.0.10.16, 4.4.15.x before 4.4.15.7, and 4.6.x before 4.6.3 allows remote attackers to conduct BBCode injection attacks against HTTP sessions via a crafted URI.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1107
5102	CVE-2016-5699	MEDIUM	Medium	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.	python	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1570
5103	CVE-2016-5696	MEDIUM	Medium	net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for man-in-the-middle attackers to hijack TCP sessions via a blind in-window attack.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1363
5104	CVE-2016-5691	HIGH	Critical	The DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact by leveraging lack of validation of (1) pixel.red, (2) pixel.green, and (3) pixel.blue.	imagemagick	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2709
5105	CVE-2016-5690	HIGH	Critical	The ReadDCMImage function in DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact via vectors involving the for statement in computing the pixel scaling table.	imagemagick	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2689
5106	CVE-2016-5689	HIGH	Critical	The DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact by leveraging lack of NULL pointer checks.	imagemagick	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2724
5107	CVE-2016-5688	MEDIUM	High	The WPG parser in ImageMagick before 6.9.4-4 and 7.x before 7.0.1-5, when a memory limit is set, allows remote attackers to have unspecified impact via vectors related to the SetImageExtent return-value check, which trigger (1) a heap-based buffer overflow in the SetPixelIndex function or an invalid write operation in the (2) ScaleCharToQuantum or (3) SetPixelIndex functions.	imagemagick	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2766
5108	CVE-2016-5687	HIGH	Critical	The VerticalFilter function in the DDS coder in ImageMagick before 6.9.4-3 and 7.x before 7.0.1-4 allows remote attackers to have unspecified impact via a crafted DDS file, which triggers an out-of-bounds read.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2722
5109	CVE-2016-5652	MEDIUM	High	An exploitable heap-based buffer overflow exists in the handling of TIFF images in LibTIFF's TIFF2PDF tool. A crafted TIFF document can lead to a heap-based buffer overflow resulting in remote code execution. Vulnerability can be triggered via a saved TIFF file delivered by other means.	libtiff	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2957
5110	CVE-2016-5636	HIGH	Critical	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow.	python	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1560
5111	CVE-2016-5635	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Security: Audit.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2168
5112	CVE-2016-5634	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to RBR.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2184
5113	CVE-2016-5633	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Performance Schema, a different vulnerability than CVE-2016-8290.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2145
5114	CVE-2016-5632	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2152
5115	CVE-2016-5631	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Memcached.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2185
5116	CVE-2016-5630	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.6.31 and earlier and 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2181
5117	CVE-2016-5629	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: Federated.	mysql	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2149
5118	CVE-2016-5628	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2186
5119	CVE-2016-5627	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.6.31 and earlier and 5.7.13 and earlier allows remote authenticated users to affect availability via vectors related to Server: InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2180
5120	CVE-2016-5626	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to GIS.	mysql	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2153
5121	CVE-2016-5625	MEDIUM	High	Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Packaging.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2157

	A	B	C	D	E	F	G	H	I	J	K	L	M
5122	CVE-2016-5624	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2171
5123	CVE-2016-5617			Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Error Handling.	mysql	Updated	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2179
5124	CVE-2016-5616			Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: MyISAM.	mysql	Updated	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2169
5125	CVE-2016-5612	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.50 and earlier, 5.6.31 and earlier, and 5.7.13 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2154
5126	CVE-2016-5609	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.6.31 and earlier and 5.7.13 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2148
5127	CVE-2016-5597	MEDIUM	Medium	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality via vectors related to Networking.	jdk&jre	Unchanged	8.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2151
5128	CVE-2016-5584	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.5.52 and earlier, 5.6.33 and earlier, and 5.7.15 and earlier allows remote administrators to affect confidentiality via vectors related to Server: Security: Encryption.	mysql	Unchanged	8.0.0.12	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2144
5129	CVE-2016-5582	HIGH	Critical	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot, a different vulnerability than CVE-2016-5573.	jdk&jre	Unchanged	8.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2141
5130	CVE-2016-5573	MEDIUM	High	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot, a different vulnerability than CVE-2016-5582.	jdk&jre	Unchanged	8.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2156
5131	CVE-2016-5568	HIGH	Critical	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, and 8u102 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT.	jdk&jre	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2172
5132	CVE-2016-5556	HIGH	Critical	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, and 8u102 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to 2D.	jdk&jre	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2174
5133	CVE-2016-5554	MEDIUM	Medium	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect integrity via vectors related to JMX.	jdk&jre	Unchanged	8.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2164
5134	CVE-2016-5552	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS v3.0 Base Score 5.3 (Integrity impacts).	jdk&jre	Unchanged	8.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3251
5135	CVE-2016-5549	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 6.5 (Confidentiality impacts).	jdk&jre	Unchanged	8.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3226

	A	B	C	D	E	F	G	H	I	J	K	L	M
5136	CVE-2016-5548	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 6.5 (Confidentiality impacts).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3315
5137	CVE-2016-5547	MEDIUM	Medium	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS v3.0 Base Score 5.3 (Availability impacts).	jdk&jre	Unchanged	8.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3221
5138	CVE-2016-5546	MEDIUM	High	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS v3.0 Base Score 7.5 (Integrity impacts).	jdk&jre	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3166
5139	CVE-2016-5542	MEDIUM	Low	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect integrity via vectors related to Libraries.	jdk&jre	Unchanged	8.0.0.12	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2142
5140	CVE-2016-5507	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.6.32 and earlier and 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2147
5141	CVE-2016-5444	MEDIUM	Low	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows remote attackers to affect confidentiality via vectors related to Server: Connection.	mysql	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1260
5142	CVE-2016-5443	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows local users to affect availability via vectors related to Server: Connection.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1253
5143	CVE-2016-5442	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Security: Encryption.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1277
5144	CVE-2016-5441	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1311
5145	CVE-2016-5440	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: RBR.	mysql	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1263
5146	CVE-2016-5439	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1298
5147	CVE-2016-5437	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Log.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1238
5148	CVE-2016-5436	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1302
5149	CVE-2016-5424	MEDIUM	High	PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 might allow remote authenticated users with the CREATEDB or CREATEROLE role to gain superuser privileges via a (1) (double quote), (2) \ (backslash), (3) carriage return, or (4) newline character in a (a) database or (b) role name that is mishandled during an administrative operation.	postgresql	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2669

	A	B	C	D	E	F	G	H	I	J	K	L	M
5150	CVE-2016-5423	MEDIUM	High	PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 allow remote authenticated users to cause a denial of service (NULL pointer dereference and server crash), obtain sensitive memory information, or possibly execute arbitrary code via (1) a CASE expression within the test value subexpression of another CASE or (2) inlining of an SQL function that implements the equality operator used for a CASE expression involving values of different types.	postgresql	Unchanged	8.0.0.13	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2750
5151	CVE-2016-5421	HIGH	Critical	Use-after-free vulnerability in libcurl before 7.50.1 allows attackers to control which connection is used or possibly have unspecified other impact via unknown vectors.	libcurl	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1398
5152	CVE-2016-5420	MEDIUM	High	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the authentication of the connection by leveraging a previously created connection with a different client certificate.	libcurl	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1413
5153	CVE-2016-5419	MEDIUM	High	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session.	libcurl	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1404
5154	CVE-2016-5418	MEDIUM	High	The sandboxing code in libarchive 3.2.0 and earlier mishandles hardlink archive entries of non-zero data size, which might allow remote attackers to write to arbitrary files via a crafted archive file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1720
5155	CVE-2016-5417	MEDIUM	High	Memory leak in the __res_vinit function in the IPv6 name server management code in libresolv in GNU C Library (aka glibc or libc6) before 2.24 allows remote attackers to cause a denial of service (memory consumption) by leveraging partial initialization of internal resolver data structures.	glibc	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3376
5156	CVE-2016-5412	MEDIUM	Medium	arch/powerpc/kvm/ book3s_hv_rmhandlers.S in the Linux kernel through 4.7 on PowerPC platforms, when CONFIG_KVM_BOOK3S_64_HV is enabled, allows guest OS users to cause a denial of service (host OS infinite loop) by making a H_CEDE hypercall during the existence of a suspended transaction.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1384
5157	CVE-2016-5408	HIGH	Critical	Stack-based buffer overflow in the munge_other_line function in cachemgr.cgi in the squid package before 3.1.23-16.el6_8.6 in Red Hat Enterprise Linux 6 allows remote attackers to execute arbitrary code via unspecified vectors. NOTE: this vulnerability exists because of an incorrect fix for CVE-2016-4051.	squid	Unchanged	Investigate	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1438
5158	CVE-2016-5407	HIGH	Critical	The (1) XvQueryAdaptors and (2) XvQueryEncodings functions in X.org libXv before 1.0.11 allow remote X servers to trigger out-of-bounds memory access operations via vectors involving length specifications in received data.	libxv	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2713
5159	CVE-2016-5403	MEDIUM	Medium	The virtqueue_pop function in hw/virtio/virtio.c in QEMU allows local guest OS administrators to cause a denial of service (memory consumption and QEMU process crash) by submitting requests without waiting for completion.	qemu	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1439
5160	CVE-2016-5400	MEDIUM	Medium	Memory leak in the airspy_probe function in drivers/media/usb/airspy/airspy.c in the airspy USB driver in the Linux kernel before 4.7 allows local users to cause a denial of service (memory consumption) via a crafted USB device that emulates many VFL_TYPE_SDR or VFL_TYPE_SUBDEV devices and performs many connect and disconnect operations.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1412
5161	CVE-2016-5399	MEDIUM	High	The bzread function in ext/bz2/bz2.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted bz2 archive.	php	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4070
5162	CVE-2016-5387	MEDIUM	High	The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an httpoxy issue. NOTE: the vendor states This mitigation has been assigned the identifier CVE-2016-5387; in other words, this is not a CVE ID for a vulnerability.	apache	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1239
5163	CVE-2016-5385	MEDIUM	High	PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, as demonstrated by (1) an application that makes a getenv('HTTP_PROXY') call or (2) a CGI configuration of PHP, aka an httpoxy issue.	php	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1305
5164	CVE-2016-5384	MEDIUM	High	fontconfig before 2.12.1 does not validate offsets, which allows local users to trigger arbitrary free calls and consequently conduct double free attacks and execute arbitrary code via a crafted cache file.	fontconfig	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1360
5165	CVE-2016-5359	MEDIUM	Medium	epan/dissectors/packet-wbxml.c in the WBXML dissector in Wireshark 1.12.x before 1.12.12 mishandles offsets, which allows remote attackers to cause a denial of service (integer overflow and infinite loop) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1411
5166	CVE-2016-5358	MEDIUM	Medium	epan/dissectors/packet-pktap.c in the Ethernet dissector in Wireshark 2.x before 2.0.4 mishandles the packet-header data type, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1358

	A	B	C	D	E	F	G	H	I	J	K	L	M
5167	CVE-2016-5357	MEDIUM	Medium	wiretap/netscreen.c in the NetScreen file parser in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles sscanf unsigned-integer processing, which allows remote attackers to cause a denial of service (application crash) via a crafted file.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1425
5168	CVE-2016-5356	MEDIUM	Medium	wiretap/cosine.c in the CoSine file parser in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles sscanf unsigned-integer processing, which allows remote attackers to cause a denial of service (application crash) via a crafted file.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1383
5169	CVE-2016-5355	MEDIUM	Medium	wiretap/toshiba.c in the Toshiba file parser in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles sscanf unsigned-integer processing, which allows remote attackers to cause a denial of service (application crash) via a crafted file.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1372
5170	CVE-2016-5354	MEDIUM	Medium	The USB subsystem in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles class types, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1401
5171	CVE-2016-5353	MEDIUM	Medium	epan/dissectors/packet-umts_fp.c in the UMTS FP dissector in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles the reserved C/T value, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1437
5172	CVE-2016-5352	MEDIUM	Medium	epan/crypt/airpdcap.c in the IEEE 802.11 dissector in Wireshark 2.x before 2.0.4 mishandles certain length values, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1408
5173	CVE-2016-5351	MEDIUM	Medium	epan/crypt/airpdcap.c in the IEEE 802.11 dissector in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles the lack of an EAPOL_RSN_KEY, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1382
5174	CVE-2016-5350	MEDIUM	High	epan/dissectors/packet-dcerpc-spoolss.c in the SPOOLS component in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles unexpected offsets, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	wireshark	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1388
5175	CVE-2016-5340	HIGH	High	The is_ashmem_file function in drivers/staging/android/ashmem.c in a certain Qualcomm Innovation Center (QuIC) Android patch for the Linux kernel 3.x mishandles pointer validation within the KGSL Linux Graphics Module, which allows attackers to bypass intended access restrictions by using the /ashmem string as the dentry name.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1374
5176	CVE-2016-5338	MEDIUM	High	The (1) esp_reg_read and (2) esp_reg_write functions in hw/scsi/esp.c in QEMU allow local guest OS administrators to cause a denial of service (QEMU process crash) or execute arbitrary code on the QEMU host via vectors related to the information transfer buffer.	qemu	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-917
5177	CVE-2016-5337	LOW	Medium	The megasas_ctrl_get_info function in hw/scsi/megasas.c in QEMU allows local guest OS administrators to obtain sensitive host memory information via vectors related to reading device control information.	qemu	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-937
5178	CVE-2016-5323	MEDIUM	High	A vulnerability was found in libtiff. A maliciously crafted TIFF file could cause the application to crash when using tiffcrop command.	libtiff	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1273
5179	CVE-2016-5322	MEDIUM	Medium	The setByteArray function in tif_dir.c in libtiff 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tiff image.	tiff	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4101
5180	CVE-2016-5321	MEDIUM	Medium	A vulnerability was found in libtiff. A maliciously crafted TIFF file could cause the application to crash when using tiffcrop command.	libtiff	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1266
5181	CVE-2016-5320			A vulnerability was found in libtiff. A maliciously crafted TIFF file could cause the application to crash or even enable RCE on vulnerable machine when using rgb2ycbcr command.?	libtiff	Updated	8.0.0.15	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3451
5182	CVE-2016-5319	MEDIUM	Medium	Heap-based buffer overflow in tif_packbits.c in libtiff 4.0.6 and earlier allows remote attackers to crash the application via a crafted bmp file.	libtiff	Unchanged	Won't Fix	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3213
5183	CVE-2016-5318	MEDIUM	Medium	Stack-based buffer overflow in the _TIFFVGetField function in libtiff 4.0.6 and earlier allows remote attackers to crash the application via a crafted tiff.	libtiff	Unchanged	8.0.0.19	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3285
5184	CVE-2016-5317	MEDIUM	Medium	Buffer overflow in the PixarLogDecode function in libtiff.so in the PixarLogDecode function in libtiff 4.0.6 and earlier, as used in GNOME nautilus, allows attackers to cause a denial of service attack (crash) via a crafted TIFF file.	libtiff	Unchanged	8.0.0.15	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3206
5185	CVE-2016-5316	MEDIUM	Medium	Out-of-bounds read in the PixarLogCleanup function in tif_pixarlog.c in libtiff 4.0.6 and earlier allows remote attackers to crash the application by sending a crafted TIFF image to the rgb2ycbcr tool.	libtiff	Unchanged	8.0.0.15	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3276
5186	CVE-2016-5315	MEDIUM	Medium	The setByteArray function in tif_dir.c in libtiff 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tiff image.	libtiff	Unchanged	8.0.0.15	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3586
5187	CVE-2016-5314	MEDIUM	HIGH	A vulnerability was found in libtiff. A maliciously crafted TIFF file could cause the application to crash when using rgb2ycbcr command.?	libtiff	Unchanged	8.0.0.15	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3452
5188	CVE-2016-5301	MEDIUM	High	The parse_chunk_header function in libtorrent before 1.1.1 allows remote attackers to cause a denial of service (crash) via a crafted (1) HTTP response or possibly a (2) UPnP broadcast.	libtorrent	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1126
5189	CVE-2016-5300	HIGH	High	The XML parser in Expat does not use sufficient entropy for hash initialization, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted identifiers in an XML document. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0876.	expat	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-936

	A	B	C	D	E	F	G	H	I	J	K	L	M
5190	CVE-2016-5244	MEDIUM	High	The rds_inc_info_copy function in net/rds/recv.c in the Linux kernel through 4.6.3 does not initialize a certain structure member, which allows remote attackers to obtain sensitive information from kernel stack memory by reading an RDS message.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-933
5191	CVE-2016-5243	LOW	Medium	The tipc_nl_compat_link_dump function in net/tipc/netlink_compat.c in the Linux kernel through 4.6.3 does not properly copy a certain string, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-930
5192	CVE-2016-5239	HIGH	Critical	The gnuplot delegate functionality in ImageMagick before 6.9.4-0 and GraphicsMagick allows remote attackers to execute arbitrary commands via unspecified vectors.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3725
5193	CVE-2016-5238	LOW	Medium	The get_cmd function in hw/scsi/esp.c in QEMU might allow local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via vectors related to reading from the information transfer buffer in non-DMA mode.	qemu	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-939
5194	CVE-2016-5195	HIGH	High	A race condition was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged, local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.	linux	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1811
5195	CVE-2016-5152	MEDIUM	High	Integer overflow in the opj_tcd_get_decoded_tile_size function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.	openjpeg	Unchanged	Won't Fix	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4552
5196	CVE-2016-5131	MEDIUM	High	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the XPointer range-to function.	libxml2	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1248
5197	CVE-2016-5126	MEDIUM	High	Heap-based buffer overflow in the iscsi_aio_ioctl function in block/iscsi.c in QEMU allows local guest OS users to cause a denial of service (QEMU process crash) or possibly execute arbitrary code via a crafted iSCSI asynchronous I/O ioctl call.	qemu	Unchanged	8.0.0.7	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-835
5198	CVE-2016-5118	HIGH	Critical	The OpenBlob function in blob.c in GraphicsMagick before 1.3.24 and ImageMagick allows remote attackers to execute arbitrary code via a | (pipe) character at the start of a filename.	imagemagick	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1452
5199	CVE-2016-5116	MEDIUM	Critical	gd_xbm.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in certain custom PHP 5.5.x configurations, allows context-dependent attackers to obtain sensitive information from process memory or cause a denial of service (stack-based buffer under-read and application crash) via a long name.	gd	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1379
5200	CVE-2016-5114	MEDIUM	Critical	sapi/fpm/fpm/fpm_log.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 misinterprets the semantics of the snprintf return value, which allows attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string, as demonstrated by a long URI in a configuration with custom REQUEST_URI logging.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1361
5201	CVE-2016-5107	LOW	Medium	The megasas_lookup_frame function in QEMU, when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds read and crash) via unspecified vectors.	qemu	Unchanged	8.0.0.10	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1569
5202	CVE-2016-5106	LOW	Medium	The megasas_dcmd_set_properties function in hw/scsi/megasas.c in QEMU, when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest administrators to cause a denial of service (out-of-bounds write access) via vectors involving a MegaRAID Firmware Interface (MFI) command.	qemu	Unchanged	8.0.0.10	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1574
5203	CVE-2016-5105	LOW	Medium	The megasas_dcmd_cfg_read function in hw/scsi/megasas.c in QEMU, when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, uses an uninitialized variable, which allows local guest administrators to read host memory via vectors involving a MegaRAID Firmware Interface (MFI) command.	qemu	Unchanged	8.0.0.10	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1571
5204	CVE-2016-5102	MEDIUM	Medium	Buffer overflow in the readgifimage function in gif2tiff.c in the gif2tiff tool in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (segmentation fault) via a crafted gif file.	libtiff	Unchanged	Won't Fix	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3198
5205	CVE-2016-5099	MEDIUM	Medium	Cross-site scripting (XSS) vulnerability in phpMyAdmin 4.4.x before 4.4.15.6 and 4.6.x before 4.6.2 allows remote attackers to inject arbitrary web script or HTML via special characters that are mishandled during double URL decoding.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1123
5206	CVE-2016-5098	MEDIUM	Medium	Directory traversal vulnerability in libraries/error_report.lib.php in phpMyAdmin before 4.6.2-prerelease allows remote attackers to determine the existence of arbitrary files by triggering an error.Per Vendor Advisory: No released version was vulnerable.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1113
5207	CVE-2016-5097	MEDIUM	Medium	phpMyAdmin before 4.6.2 places tokens in query strings and does not arrange for them to be stripped before external navigation, which allows remote attackers to obtain sensitive information by reading (1) HTTP requests or (2) server logs.	phpmyadmin	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1114
5208	CVE-2016-5096	HIGH	High	Integer overflow in the fread function in ext/standard/file.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer in the second argument.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1432

	A	B	C	D	E	F	G	H	I	J	K	L	M
5209	CVE-2016-5095	HIGH	High	Integer overflow in the php_escape_html_entities_ex function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from a FILTER_SANITIZE_FULL_SPECIAL_CHARS filter_var call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-5094.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1414
5210	CVE-2016-5094	HIGH	High	Integer overflow in the php_html_entities function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from the htmlspecialchars function.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1423
5211	CVE-2016-5093	HIGH	High	The get_icu_value_internal function in ext/intl/locale/locale_methods.c in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 does not ensure the presence of a '\0' character, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted locale_get_primary_language call.	php	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1424
5212	CVE-2016-5011	MEDIUM	Medium	By connecting a storage medium containing a specially crafted MBR a local user can cause a Linux system to become unresponsive.	util-linux	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1691
5213	CVE-2016-5010	MEDIUM	Medium	coders/tiff.c in ImageMagick before 6.9.5-3 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TIFF file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4014
5214	CVE-2016-5008	MEDIUM	Critical	libvirt before 2.0.0 improperly disables password checking when the password on a VNC server is set to an empty string, which allows remote attackers to bypass authentication and establish a VNC session by connecting to the server.	libvirt	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1272
5215	CVE-2016-4998	MEDIUM	High	An out-of-bounds heap memory access, leading to a Denial of Service or possibly heap disclosure or further impact was found in setsockopt(). The particular setsockopt() call is normally restricted to root, however some processes with cap_sys_admin may also be able to trigger this flaw.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-946
5216	CVE-2016-4997	HIGH	High	A flaw was discovered in processing setsockopt for 32 bit processes on 64 bit systems. This flaw will allow attackers to alter arbitrary kernel memory when unloading a kernel module. This action is usually restricted to root-privileged users but can also be leveraged if the kernel is compiled with CONFIG_USER_NS and CONFIG_NET_NS and the user is granted elevated privileges.	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-945
5217	CVE-2016-4979	MEDIUM	High	The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the SSLVerifyClient require directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.	apache	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1120
5218	CVE-2016-4975	MEDIUM	MEDIUM	Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the Location or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).	apache	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4540
5219	CVE-2016-4973	MEDIUM	High	Binaries compiled against targets that use the libssp library in GCC for stack smashing protection (SSP) might allow local users to perform buffer overflow attacks by leveraging lack of the Object Size Checking feature.	gcc	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4378
5220	CVE-2016-4971	MEDIUM	High	GNU wget before 1.18 allows remote servers to write to arbitrary files by redirecting a request from HTTP to a crafted FTP resource.	wget	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1099
5221	CVE-2016-4964	MEDIUM	Medium	The mptsas_fetch_requests function in hw/scsi/mptsas.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop, and CPU consumption or QEMU process crash) via vectors involving s->state.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2733
5222	CVE-2016-4957	MEDIUM	High	The fix for Sec 3007 in ntp-4.2.8p7 contained a bug that could cause ntpd to crash.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-844
5223	CVE-2016-4956	MEDIUM	Medium	The fix for NtpBug2978 does not cover broadcast associations, so broadcast clients can be triggered to flip into interleave mode.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-838
5224	CVE-2016-4955	LOW	Medium	An attacker who is able to spoof a packet with a correct origin timestamp before the expected response packet arrives at the target machine can send a CRYPTO_NAK or a bad MAC and cause the association's peer variables to be cleared. If this can be done often enough, it will prevent that association from working.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-833
5225	CVE-2016-4954	MEDIUM	Medium	An attacker who is able to spoof packets with correct origin timestamps from enough servers before the expected response packets arrive at the target machine can affect some peer variables and, for example, cause a false leap indication to be set.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-818
5226	CVE-2016-4953	MEDIUM	Medium	It was found that the fixes for CVE-2015-7979 and CVE-2016-1547 were incomplete: An attacker can send a spoofed packet that contains an invalid MAC to a client/peer and demobilize its ephemeral association.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-849
5227	CVE-2016-4952	LOW	Medium	QEMU (aka Quick Emulator), when built with VMWARE PVSCSI paravirtual SCSI bus emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds array access) via vectors related to the (1) PVSCSI_CMD_SETUP_RINGS or (2) PVSCSI_CMD_SETUP_MSG_RING SCSI command.	qemu	Unchanged	8.0.0.10	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1562

	A	B	C	D	E	F	G	H	I	J	K	L	M
5228	CVE-2016-4951	HIGH	High	The tipc_nl_publ_dump function in net/tipc/socket.c in the Linux kernel through 4.6 does not verify socket existence, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a dumpit operation.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-763
5229	CVE-2016-4913	HIGH	High	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem.	linux	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-767
5230	CVE-2016-4809	MEDIUM	High	The archive_read_format_cpio_read_header function in archive_read_support_format_cpio.c in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) via a CPIO archive with a large symlink.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1741
5231	CVE-2016-4805	HIGH	High	Use-after-free vulnerability in drivers/net/ppp/ppp_generic.c in the Linux kernel before 4.5.2 allows local users to cause a denial of service (memory corruption and system crash, or spinlock) or possibly have unspecified other impact by removing a network namespace, related to the ppp_register_net_channel and ppp_unregister_channel functions.CWE-416: Use After Free	linux	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-781
5232	CVE-2016-4804	LOW	Medium	The read_boot function in boot.c in dosfstools before 4.0 allows attackers to cause a denial of service (crash) via a crafted filesystem, which triggers a heap-based buffer overflow in the (1) read_fat function or an out-of-bounds heap read in (2) get_fat function.	dosfstools	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-812
5233	CVE-2016-4802	MEDIUM	High	Multiple untrusted search path vulnerabilities in cURL and libcurl before 7.49.1, when built with SSPI or telnet is enabled, allow local users to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse (1) security.dll, (2) secur32.dll, or (3) ws2_32.dll in the application or current working directory.	curl	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-925
5234	CVE-2016-4797	MEDIUM	Medium	Divide-by-zero vulnerability in the opj_tcd_init_tile function in tcd.c in OpenJPEG before 2.1.1 allows remote attackers to cause a denial of service (application crash) via a crafted jp2 file. NOTE: this issue exists because of an incorrect fix for CVE-2014-7947.	openjpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3306
5235	CVE-2016-4796	MEDIUM	Medium	Heap-based buffer overflow in the color_cmyk_to_rgb in common/color.c in OpenJPEG before 2.1.1 allows remote attackers to cause a denial of service (crash) via a crafted .j2k file.	openjpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3252
5236	CVE-2016-4794	HIGH	High	Use-after-free vulnerability in mm/percpu.c in the Linux kernel through 4.6 allows local users to cause a denial of service (BUG) or possibly have unspecified other impact via crafted use of the mmap and bpf system calls.CWE-416: Use After Free	linux	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-757
5237	CVE-2016-4761	HIGH	CRITICAL	WebKitGTK+ before 2.14.0: A use-after-free vulnerability can allow remote attackers to cause a DoS	webkitgtk	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-4052
5238	CVE-2016-4657	MEDIUM	High	WebKit in Apple iOS before 9.3.5 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1507
5239	CVE-2016-4624	MEDIUM	High	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4589, CVE-2016-4622, and CVE-2016-4623.	webkit	Unchanged	Vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1278
5240	CVE-2016-4623	MEDIUM	High	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4589, CVE-2016-4622, and CVE-2016-4624.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1257
5241	CVE-2016-4622	MEDIUM	High	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4589, CVE-2016-4623, and CVE-2016-4624.	webkit	Unchanged	Vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1265
5242	CVE-2016-4619			libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4614, CVE-2016-4615, and CVE-2016-4616.	libxml2	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1267
5243	CVE-2016-4616	HIGH	Critical	libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4614, CVE-2016-4615, and CVE-2016-4619.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1291
5244	CVE-2016-4615	HIGH	Critical	libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4614, CVE-2016-4616, and CVE-2016-4619.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1256

	A	B	C	D	E	F	G	H	I	J	K	L	M
5245	CVE-2016-4614	HIGH	Critical	libxml2 in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4615, CVE-2016-4616, and CVE-2016-4619.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1245
5246	CVE-2016-4612			libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4607, CVE-2016-4608, CVE-2016-4609, and CVE-2016-4610.	libxslt	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1262
5247	CVE-2016-4610	HIGH	Critical	libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4607, CVE-2016-4608, CVE-2016-4609, and CVE-2016-4612.	libxslt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1251
5248	CVE-2016-4609	HIGH	Critical	libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4607, CVE-2016-4608, CVE-2016-4610, and CVE-2016-4612.	libxslt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1280
5249	CVE-2016-4608	HIGH	Critical	libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4607, CVE-2016-4609, CVE-2016-4610, and CVE-2016-4612.	libxslt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1286
5250	CVE-2016-4607	HIGH	Critical	libxslt in Apple iOS before 9.3.3, OS X before 10.11.6, iTunes before 12.4.2 on Windows, iCloud before 5.2.1 on Windows, tvOS before 9.2.2, and watchOS before 2.2.2 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2016-4608, CVE-2016-4609, CVE-2016-4610, and CVE-2016-4612.	libxslt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1261
5251	CVE-2016-4592	HIGH	Medium	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to cause a denial of service (memory consumption) via a crafted web site.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1307
5252	CVE-2016-4591	HIGH	High	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 mishandles the location variable, which allows remote attackers to access the local filesystem via unspecified vectors.	webkit	Unchanged	Vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1244
5253	CVE-2016-4590	MEDIUM	Medium	WebKit in Apple iOS before 9.3.3 and Safari before 9.1.2 mishandles about: URLs, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.	webkit	Unchanged	Vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1292
5254	CVE-2016-4589	MEDIUM	High	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4622, CVE-2016-4623, and CVE-2016-4624.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1312
5255	CVE-2016-4588	MEDIUM	High	WebKit in Apple tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1297
5256	CVE-2016-4587	MEDIUM	Medium	WebKit in Apple iOS before 9.3.3 and tvOS before 9.2.2 allows remote attackers to obtain sensitive information from uninitialized process memory via a crafted web site.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1255
5257	CVE-2016-4586	MEDIUM	High	WebKit in Apple Safari before 9.1.2 and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1279
5258	CVE-2016-4585	MEDIUM	Medium	Cross-site scripting (XSS) vulnerability in the WebKit Page Loading implementation in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to inject arbitrary web script or HTML via an HTTP response specifying redirection that is mishandled by Safari.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1304
5259	CVE-2016-4584	MEDIUM	High	The WebKit Page Loading implementation in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1294
5260	CVE-2016-4583	MEDIUM	Medium	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to bypass the Same Origin Policy and obtain image date from an unintended web site via a timing attack involving an SVG document.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1252
5261	CVE-2016-4581	MEDIUM	Medium	fs/pnode.c in the Linux kernel before 4.5.4 does not properly traverse a mount propagation tree in a certain case involving a slave mount, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted series of mount system calls.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-759
5262	CVE-2016-4580	MEDIUM	High	The x25_negotiate_facilities function in net/x25/x25_facilities.c in the Linux kernel before 4.5.5 does not properly initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack memory via an X.25 Call Request.	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-768

	A	B	C	D	E	F	G	H	I	J	K	L	M
5263	CVE-2016-4578	LOW	Medium	sound/core/timer.c in the Linux kernel through 4.6 does not initialize certain r1 data structures, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface, related to the (1) snd_timer_user_ccallback and (2) snd_timer_user_tinterrupt functions.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-725
5264	CVE-2016-4569	LOW	Medium	The snd_timer_user_params function in sound/core/timer.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-739
5265	CVE-2016-4568	HIGH	High	drivers/media/v4l2-core/videobuf2-v4l2.c in the Linux kernel before 4.5.3 allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a crafted number of planes in a VIDIOC_DQBUF ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-730
5266	CVE-2016-4565	HIGH	High	The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a uAPI interface.	linux	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-724
5267	CVE-2016-4564	HIGH	Critical	The DrawImage function in MagickCore/draw.c in ImageMagick before 6.9.4-0 and 7.x before 7.0.1-2 makes an incorrect function call in attempting to locate the next token, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted file.	imagemagick	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-820
5268	CVE-2016-4563	MEDIUM	High	The TraceStrokePolygon function in MagickCore/draw.c in ImageMagick before 6.9.4-0 and 7.x before 7.0.1-2 mishandles the relationship between the BezierQuantum value and certain stroke data, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted file.	imagemagick	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-814
5269	CVE-2016-4562	MEDIUM	High	The DrawDashPolygon function in MagickCore/draw.c in ImageMagick before 6.9.4-0 and 7.x before 7.0.1-2 mishandles calculations of certain vertices integer data, which allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted file.	imagemagick	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-846
5270	CVE-2016-4558	MEDIUM	High	The BPF subsystem in the Linux kernel before 4.5.5 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted application on (1) a system with more than 32 Gb of memory, related to the program reference count or (2) a 1 Tb system, related to the map reference count.CWE-416: Use After Free	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-741
5271	CVE-2016-4557	HIGH	High	The replace_map_fd_with_map_ptr function in kernel/bpf/verifier.c in the Linux kernel before 4.5.5 does not properly maintain an fd data structure, which allows local users to gain privileges or cause a denial of service (use-after-free) via crafted BPF instructions that reference an incorrect file descriptor.CWE-416: Use After Free	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-754
5272	CVE-2016-4556	MEDIUM	High	Double free vulnerability in Esi.cc in Squid 3.x before 3.5.18 and 4.x before 4.0.10 allows remote servers to cause a denial of service (crash) via a crafted Edge Side Includes (ESI) response.	squid	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-579
5273	CVE-2016-4555	MEDIUM	High	client_side_request.cc in Squid 3.x before 3.5.18 and 4.x before 4.0.10 allows remote servers to cause a denial of service (crash) via crafted Edge Side Includes (ESI) responses.	squid	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-647
5274	CVE-2016-4554	MEDIUM	High	mime_header.cc in Squid before 3.5.18 allows remote attackers to bypass intended same-origin restrictions and possibly conduct cache-poisoning attacks via a crated HTTP Host header, aka a header smuggling issue.	squid	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-609
5275	CVE-2016-4553	MEDIUM	High	client_side.cc in Squid before 3.5.18 and 4.x before 4.0.10 does not properly ignore the Host header when absolute-URI is provided, which allows remote attackers to conduct cache-poisoning attacks via an HTTP request.	squid	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-566
5276	CVE-2016-4544	HIGH	Critical	The exif_process_TIFF_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate TIFF start data, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-715
5277	CVE-2016-4543	HIGH	Critical	The exif_process_IFD_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate IFD sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-779
5278	CVE-2016-4542	HIGH	Critical	The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.CWE-125: Out-of-bounds Read	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-750

	A	B	C	D	E	F	G	H	I	J	K	L	M
5279	CVE-2016-4541	HIGH	Critical	The grapheme_strpos function in ext/intl/grapheme/grapheme_string.c in before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.CWE-125: Out-of-bounds Read	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-727
5280	CVE-2016-4540	HIGH	Critical	The grapheme_stripos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.CWE-125: Out-of-bounds Read	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-773
5281	CVE-2016-4539	HIGH	Critical	The xml_parse_into_struct function in ext/xml/xml.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted XML data in the second argument, leading to a parser level of zero.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-752
5282	CVE-2016-4538	HIGH	Critical	The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 modifies certain data structures without considering whether they are copies of the _zero_, _one_, or _two_ global variable, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-714
5283	CVE-2016-4537	HIGH	Critical	The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 accepts a negative integer for the scale argument, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-769
5284	CVE-2016-4493	MEDIUM	Medium	The demangle_template_value_parm and do_hpacc_template_literal functions in cplus-dem.c in libiberty allow remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted binary.	gcc	Unchanged	8.0.0.23	9.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5197
5285	CVE-2016-4492	MEDIUM	Medium	Buffer overflow in the do_type function in cplus-dem.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary.	gcc	Unchanged	8.0.0.23	9.0.0.21	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5196
5286	CVE-2016-4491	MEDIUM	Medium	The d_print_comp function in cp-demangle.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, which triggers infinite recursion and a buffer overflow, related to a node having itself as ancestor more than once.	gcc	Unchanged	8.0.0.23	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5195
5287	CVE-2016-4490	MEDIUM	Medium	A vulnerability was found in gcc. Due to the inconsistent use of long and int for string/array length in cp-demangle.c there is an integer overflow that leads to a write access violation. The target crashes on an access violation at an address matching the destination operand of the instruction.	gcc	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-681
5288	CVE-2016-4489	MEDIUM	Medium	A vulnerability was found in gcc. It's possible to achieve an invalid write of size 8 due to an integer overflow in the demangling of virtual tables in method gnu_special.	gcc	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-679
5289	CVE-2016-4488	MEDIUM	Medium	A vulnerability was found in gcc. There is a variable ksize storing the amount of allocated memory for the array ktypevec. ksize being zero (0) indicates that some memory must be allocated upon the first write. When more memory is needed, both ksize and the memory are doubled during reallocation. At some point the memory for the array is freed (in squangle_mop_up) but the value of ksize remains. Since ksize is not 0, there is no indication that new memory must be allocated when there is another write to the array. This allows a malicious attacker to write arbitrary content to freed memory.	gcc	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-678
5290	CVE-2016-4487	MEDIUM	Medium	Use-after-free vulnerability in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to btypevec.	gcc	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5194
5291	CVE-2016-4486	LOW	Low	The rtnl_fill_link_ifmap function in net/core/rtnetlink.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-722
5292	CVE-2016-4485	MEDIUM	High	The llc_cmsg_rcv function in net/llc/af_llc.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack memory by reading a message.	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-756
5293	CVE-2016-4484	HIGH	Medium	The Debian initrd script for the cryptsetup package 2:1.7.3-2 and earlier allows physically proximate attackers to gain shell access via many log in attempts with an invalid password.	cryptsetup	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3188
5294	CVE-2016-4483	MEDIUM	High	A vulnerability was found in libxml2. Parsing a maliciously crafted xml file could cause the application to crash if recover mode is used.	libxml2	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1458
5295	CVE-2016-4482	LOW	Medium	The proc_connectinfo function in drivers/usb/core/devio.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted USBDEVFS_CONNECTINFO ioctl call.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-766
5296	CVE-2016-4477	MEDIUM	High	wpa_supplicant 0.4.0 through 2.5 does not reject \n and \r characters in passphrase parameters, which allows local users to trigger arbitrary library loading and consequently gain privileges, or cause a denial of service (daemon outage), via a crafted (1) SET, (2) SET_CRED, or (3) SET_NETWORK command.	wpa_supplicant	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-600

	A	B	C	D	E	F	G	H	I	J	K	L	M
5297	CVE-2016-4476	MEDIUM	High	hostapd 0.6.7 through 2.5 and wpa_supplicant 0.6.7 through 2.5 do not reject \n and \r characters in passphrase parameters, which allows remote attackers to cause a denial of service (daemon outage) via a crafted WPS operation.	Hostapd & wpa_supplicant	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-585
5298	CVE-2016-4473	HIGH	Critical	/ext/phar/phar_object.c in PHP 7.0.7 and 5.6.x allows remote attackers to execute arbitrary code. NOTE: Introduced as part of an incomplete fix to CVE-2015-6833.	php	Unchanged	8.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4412
5299	CVE-2016-4472	MEDIUM	High	The overflow protection in Expat is removed by compilers with certain optimization settings, which allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via crafted XML data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1283 and CVE-2015-2716.	expat	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1128
5300	CVE-2016-4470	MEDIUM	Medium	The key_reject_and_link function in security/keys/key.c in the Linux kernel through 4.6.3 does not ensure that a certain data structure is initialized, which allows local users to cause a denial of service (system crash) via vectors involving a crafted keyctl request2 command.CWE-416: Use After Free	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-940
5301	CVE-2016-4463	MEDIUM	High	Stack-based buffer overflow in Apache Xerces-C++ before 3.1.4 allows context-dependent attackers to cause a denial of service via a deeply nested DTD.	xerces-c	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1108
5302	CVE-2016-4456	MEDIUM	High	The GNUTLS_KEYLOGFILE environment variable in gnutls 3.4.12 allows remote attackers to overwrite and corrupt arbitrary files in the filesystem.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5078
5303	CVE-2016-4454	LOW	Medium	The vmsvga_fifo_read_raw function in hw/display/vmware_vga.c in QEMU allows local guest OS administrators to obtain sensitive host memory information or cause a denial of service (QEMU process crash) by changing FIFO registers and issuing a VGA command, which triggers an out-of-bounds read.	qemu	Unchanged	8.0.0.7	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-841
5304	CVE-2016-4453	MEDIUM	Medium	The vmsvga_fifo_run function in hw/display/vmware_vga.c in QEMU allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via a VGA command.	qemu	Unchanged	8.0.0.7	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-823
5305	CVE-2016-4450	MEDIUM	High	os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.CWE-476: NULL Pointer Dereference	nginx	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-816
5306	CVE-2016-4449	MEDIUM	High	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors.	libxml2	Unchanged	8.0.0.7	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-815
5307	CVE-2016-4448	HIGH	Critical	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.	libxml2	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-828
5308	CVE-2016-4447	MEDIUM	High	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName.	libxml2	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-829
5309	CVE-2016-4441	LOW	Medium	The get_cmd function in hw/scsi/esp.c in the 53C9X Fast SCSI Controller (FSC) support in QEMU does not properly check DMA length, which allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via unspecified vectors, involving an SCSI command.	qemu	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-755
5310	CVE-2016-4440	HIGH	High	arch/x86/kvm/vmx.c in the Linux kernel through 4.6.3 mishandles the APICv on/off state, which allows guest OS users to obtain direct APIC MSR access on the host OS, and consequently cause a denial of service (host OS crash) or possibly execute arbitrary code on the host OS, via x2APIC mode.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-929
5311	CVE-2016-4439	MEDIUM	High	The esp_reg_write function in hw/scsi/esp.c in the 53C9X Fast SCSI Controller (FSC) support in QEMU does not properly check command buffer length, which allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) or potentially execute arbitrary code on the QEMU host via unspecified vectors.	qemu	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-761
5312	CVE-2016-4429	HIGH	Critical	Stack-based buffer overflow in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) allows remote servers to cause a denial of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets.	glibc	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-847
5313	CVE-2016-4421	MEDIUM	Medium	epan/dissectors/packet-ber.c in the ASN.1 BER dissector in Wireshark 1.12.x before 1.12.10 and 2.x before 2.0.2 allows remote attackers to cause a denial of service (deep recursion, stack consumption, and application crash) via a packet that specifies deeply nested data.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-603
5314	CVE-2016-4420	MEDIUM	Medium	The NFS dissector in Wireshark 2.x before 2.0.2 allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-671
5315	CVE-2016-4419	MEDIUM	Medium	epan/dissectors/packet-spice.c in the SPICE dissector in Wireshark 2.x before 2.0.2 mishandles capability data, which allows remote attackers to cause a denial of service (large loop) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-660
5316	CVE-2016-4418	MEDIUM	Medium	epan/dissectors/packet-ber.c in the ASN.1 BER dissector in Wireshark 1.12.x before 1.12.10 and 2.x before 2.0.2 allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted packet that triggers an empty set.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-593

	A	B	C	D	E	F	G	H	I	J	K	L	M
5317	CVE-2016-4417	MEDIUM	Medium	Off-by-one error in epan/dissectors/packet-gsm_abis_oml.c in the GSM A-bis OML dissector in Wireshark 1.12.x before 1.12.10 and 2.x before 2.0.2 allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted packet that triggers a 0xff tag value.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-646
5318	CVE-2016-4416	MEDIUM	Medium	epan/dissectors/packet-ieee80211.c in the IEEE 802.11 dissector in Wireshark 2.x before 2.0.2 mishandles the Grouping subfield, which allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-588
5319	CVE-2016-4415	MEDIUM	Medium	wiretap/vwr.c in the Ixia IxVeriWave file parser in Wireshark 2.x before 2.0.2 incorrectly increases a certain octet count, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) via a crafted file.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-628
5320	CVE-2016-4412	LOW	Medium	An issue was discovered in phpMyAdmin. A user can be tricked into following a link leading to phpMyAdmin, which after authentication redirects to another malicious site. The attacker must sniff the user's valid phpMyAdmin token. All 4.0.x versions (prior to 4.0.10.16) are affected.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2742
5321	CVE-2016-4352	MEDIUM	Medium	Integer overflow in the demuxer function in libmpdemux/demux_gif.c in Mplayer allows remote attackers to cause a denial of service (crash) via large dimensions in a gif file.	mplayer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3239
5322	CVE-2016-4348	MEDIUM	High	The _rsvg_css_normalize_font_size function in librsvg 2.40.2 allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via circular definitions in an SVG document.	librsvg	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-711
5323	CVE-2016-4346	HIGH	Critical	Integer overflow in the str_pad function in ext/standard/string.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-771
5324	CVE-2016-4345	HIGH	Critical	Integer overflow in the php_filter_encode_url function in ext/filter/sanitizing_filters.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-787
5325	CVE-2016-4344	HIGH	Critical	Integer overflow in the xml_utf8_encode function in ext/xml/xml.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long argument to the utf8_encode function, leading to a heap-based buffer overflow.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-734
5326	CVE-2016-4343	MEDIUM	High	The phar_make_dirstream function in ext/phar/dirstream.c in PHP before 5.6.18 and 7.x before 7.0.3 mishandles zero-size ./.@LongLink files, which allows remote attackers to cause a denial of service (uninitialized pointer dereference) or possibly have unspecified other impact via a crafted TAR archive.CWE-824: Access of Uninitialized Pointer	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-782
5327	CVE-2016-4342	HIGH	High	ext/phar/phar_object.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 mishandles zero-length uncompressed data, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted (1) TAR, (2) ZIP, or (3) PHAR archive.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-749
5328	CVE-2016-4323	MEDIUM	Low	A directory traversal exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent from the server could potentially result in an overwrite of files. A malicious server or someone with access to the network traffic can provide an invalid filename for a splash image triggering the vulnerability.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2961
5329	CVE-2016-4303	HIGH	Critical	The parse_string function in cjson.c in the cJSON library mishandles UTF8/16 strings, which allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a non-hex character in a JSON string, which triggers a heap-based buffer overflow.	iperf	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1745
5330	CVE-2016-4302	MEDIUM	High	Heap-based buffer overflow in the parse_codes function in archive_read_support_format_rar.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a RAR file with a zero-sized dictionary.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1751
5331	CVE-2016-4301	MEDIUM	High	Stack-based buffer overflow in the parse_device function in archive_read_support_format_mtree.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a crafted mtree file.	libarchive	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1723
5332	CVE-2016-4300	MEDIUM	High	Integer overflow in the read_SubStreamsInfo function in archive_read_support_format_7zip.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a 7zip file with a large number of substreams, which triggers a heap-based buffer overflow.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1755
5333	CVE-2016-4085	MEDIUM	Medium	Stack-based buffer overflow in epan/dissectors/packet-ncp2222.inc in the NCP dissector in Wireshark 1.12.x before 1.12.11 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a long string in a packet.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-649
5334	CVE-2016-4084	MEDIUM	Medium	Integer signedness error in epan/dissectors/packet-mswsp.c in the MS-WSP dissector in Wireshark 2.0.x before 2.0.3 allows remote attackers to cause a denial of service (integer overflow and application crash) via a crafted packet that triggers an unexpected array size.CWE-190: Integer Overflow or Wraparound	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-670

	A	B	C	D	E	F	G	H	I	J	K	L	M
5335	CVE-2016-4083	MEDIUM	Medium	epan/dissectors/packet-mswsp.c in the MS-WSP dissector in Wireshark 2.0.x before 2.0.3 does not ensure that data is available before array allocation, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-572
5336	CVE-2016-4082	MEDIUM	Medium	epan/dissectors/packet-gsm_cbch.c in the GSM CBCH dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 uses the wrong variable to index an array, which allows remote attackers to cause a denial of service (out-of-bounds access and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-586
5337	CVE-2016-4081	MEDIUM	Medium	epan/dissectors/packet-iax2.c in the IAX2 dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 uses an incorrect integer data type, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-599
5338	CVE-2016-4080	MEDIUM	Medium	epan/dissectors/packet-pktc.c in the PKTC dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 misparses timestamp fields, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-589
5339	CVE-2016-4079	MEDIUM	Medium	epan/dissectors/packet-pktc.c in the PKTC dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 does not verify BER identifiers, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-651
5340	CVE-2016-4078	MEDIUM	Medium	The IEEE 802.11 dissector in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 does not properly restrict element lists, which allows remote attackers to cause a denial of service (deep recursion and application crash) via a crafted packet, related to epan/dissectors/packet-capwap.c and epan/dissectors/packet-ieee80211.c.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-580
5341	CVE-2016-4077	MEDIUM	Medium	epan/reassemble.c in TShark in Wireshark 2.0.x before 2.0.3 relies on incorrect special-case handling of truncated Tvb data structures, which allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted packet.CWE-416: Use After Free	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-596
5342	CVE-2016-4076	MEDIUM	Medium	epan/dissectors/packet-ncp2222.inc in the NCP dissector in Wireshark 2.0.x before 2.0.3 does not properly initialize memory for search patterns, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-615
5343	CVE-2016-4074	HIGH	High	The jv_dump_term function in jq 1.5 allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted JSON file.	jq	Unchanged	Vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-619
5344	CVE-2016-4073	HIGH	Critical	Multiple integer overflows in the mbfl_strcut function in ext/mbstring/libmbfl/mbfl/mbfilter.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted mb_strcut call.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-718
5345	CVE-2016-4072	HIGH	Critical	The Phar extension in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via a crafted filename, as demonstrated by mishandling of \0 characters by the phar_analyze_path function in ext/phar/phar.c.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-772
5346	CVE-2016-4071	HIGH	Critical	Format string vulnerability in the php_snmp_error function in ext/snmp/snmp.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via format string specifiers in an SNMP::get call.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-744
5347	CVE-2016-4070	MEDIUM	High	** DISPUTED ** Integer overflow in the php_raw_url_encode function in ext/standard/url.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to cause a denial of service (application crash) via a long string to the rawurlencode function. NOTE: the vendor says Not sure if this qualifies as security issue (probably not).	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-770
5348	CVE-2016-4054	MEDIUM	High	Buffer overflow in Squid 3.x before 3.5.17 and 4.x before 4.0.9 allows remote attackers to execute arbitrary code via crafted Edge Side Includes (ESI) responses.	squid	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-644
5349	CVE-2016-4053	MEDIUM	Low	Squid 3.x before 3.5.17 and 4.x before 4.0.9 allow remote attackers to obtain sensitive stack layout information via crafted Edge Side Includes (ESI) responses, related to incorrect use of assert and compiler optimization.	squid	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-563
5350	CVE-2016-4052	MEDIUM	High	Multiple stack-based buffer overflows in Squid 3.x before 3.5.17 and 4.x before 4.0.9 allow remote HTTP servers to cause a denial of service or execute arbitrary code via crafted Edge Side Includes (ESI) responses.	squid	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-673
5351	CVE-2016-4051	MEDIUM	High	Buffer overflow in cachemgr.cgi in Squid 2.x, 3.x before 3.5.17, and 4.x before 4.0.9 might allow remote attackers to cause a denial of service or execute arbitrary code by seeding manager reports with crafted data.	squid	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-605
5352	CVE-2016-4049	MEDIUM	High	The bgp_dump_routes_func function in bgpd/bgp_dump.c in Quagga does not perform size checks when dumping data, which might allow remote attackers to cause a denial of service (assertion failure and daemon crash) via a large BGP packet.	quagga	Unchanged	8.0.0.26	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-707
5353	CVE-2016-4037	MEDIUM	Medium	The ehci_advance_state function in hw/usb/hcd-ehci.c in QEMU allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) via a circular split isochronous transfer descriptor (siTD) list, a related issue to CVE-2015-8558.	qemu	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-776
5354	CVE-2016-4024	HIGH	Critical	Integer overflow in imlib2 before 1.4.9 on 32-bit platforms allows remote attackers to execute arbitrary code via large dimensions in an image, which triggers an out-of-bounds heap memory write operation.	imlib2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-650

	A	B	C	D	E	F	G	H	I	J	K	L	M
5355	CVE-2016-4020	LOW	Medium	The patch_instruction function in hw/i386/kvmvapic.c in QEMU does not initialize the imm32 variable, which allows local guest OS administrators to obtain sensitive information from host stack memory by accessing the Task Priority Register (TPR).	qemu	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-745
5356	CVE-2016-4008	MEDIUM	Medium	The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.8, when used without the ASN1_DECODE_FLAG_STRICT_DER flag, allows remote attackers to cause a denial of service (infinite recursion) via a crafted certificate.	libtasn1	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-581
5357	CVE-2016-4006	MEDIUM	Medium	epan/proto.c in Wireshark 1.12.x before 1.12.11 and 2.0.x before 2.0.3 does not limit the protocol-tree depth, which allows remote attackers to cause a denial of service (stack memory consumption and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-657
5358	CVE-2016-4002	MEDIUM	Critical	Buffer overflow in the mipsnet_receive function in hw/net/mipsnet.c in QEMU, when the guest NIC is configured to accept large packets, allows remote attackers to cause a denial of service (memory corruption and QEMU crash) or possibly execute arbitrary code via a packet larger than 1514 bytes.	qemu	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-631
5359	CVE-2016-4001	MEDIUM	Medium	Buffer overflow in the stellaris_enet_receive function in hw/net/stellaris_enet.c in QEMU, when the Stellaris ethernet controller is configured to accept large packets, allows remote attackers to cause a denial of service (QEMU crash) via a large packet.	qemu	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-764
5360	CVE-2016-3994	MEDIUM	High	The GIF loader in imlib2 before 1.4.9 allows remote attackers to cause a denial of service (application crash) or obtain sensitive information via a crafted image, which triggers an out-of-bounds read.	imlib2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-584
5361	CVE-2016-3993	MEDIUM	High	Off-by-one error in the __imlib_MergeUpdate function in lib/updates.c in imlib2 before 1.4.9 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted coordinates.	imlib2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-653
5362	CVE-2016-3991	MEDIUM	High	Heap-based buffer overflow in the loadImage function in the tiffcrop tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image with zero tiles.	libtiff	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1736
5363	CVE-2016-3990	MEDIUM	High	Heap-based buffer overflow in the horizontalDifference8 function in tif_pixarlog.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image to tiffcp.	libtiff	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1715
5364	CVE-2016-3977	MEDIUM	Medium	Heap-based buffer overflow in util/gif2rgb.c in gif2rgb in giflib 5.1.2 allows remote attackers to cause a denial of service (application crash) via the background color index in a GIF file.	giflib	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-481
5365	CVE-2016-3961	LOW	Medium	Xen and the Linux kernel through 4.5.x do not properly suppress hugetlbfs support in x86 PV guests, which allows local PV guest users to cause a denial of service (guest OS crash) by attempting to access a hugetlbfs mapped area.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-521
5366	CVE-2016-3955	HIGH	Critical	Linux kernel built with the USB over IP(CONFIG_USBIP_*) support is vulnerable to a buffer overflow issue. It could occur while receiving USB/IP packets, when the size value in the packet is greater actual transfer buffer. A user/process could use this flaw to crash the remote host via kernel memory corruption or potentially execute arbitrary code.	linux	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-944
5367	CVE-2016-3951	MEDIUM	Medium	The bug allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have other impact by inserting a USB device with an invalid USB descriptor.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-501
5368	CVE-2016-3948	MEDIUM	High	Squid 3.x before 3.5.16 and 4.x before 4.0.8 improperly perform bounds checking, which allows remote attackers to cause a denial of service via a crafted HTTP response, related to Vary headers.	squid	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-433
5369	CVE-2016-3947	HIGH	High	Heap-based buffer overflow in the Icmp6::Recv function in icmp/Icmp6.cc in the pinger in Squid before 3.5.16 and 4.x before 4.0.8 allows remote servers to cause a denial of service (performance degradation or transition failures) or write sensitive information to log files via an ICMPv6 packet.	squid	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-443
5370	CVE-2016-3945	MEDIUM	High	Multiple integer overflows in the (1) cvt_by_strip and (2) cvt_by_tile functions in the tiff2rgba tool in LibTIFF 4.0.6 and earlier, when -b mode is enabled, allow remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image, which triggers an out-of-bounds write.	libtiff	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1749
5371	CVE-2016-3857	HIGH	High	The kernel in Android before 2016-08-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 28522518.	linux	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4176
5372	CVE-2016-3841	HIGH	High	The IPv6 stack in the Linux kernel before 4.3.3 mishandles options data, which allows local users to gain privileges or cause a denial of service (use-after-free and system crash) via a crafted sendmsg system call.	linux	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1381
5373	CVE-2016-3739	LOW	Medium	The (1) mbed_connect_step1 function in lib/vtls/mbedtls.c and (2) polarssl_connect_step1 function in lib/vtls/polarssl.c in cURL and libcurl before 7.49.0, when using SSLv3 or making a TLS connection to a URL that uses a numerical IP address, allow remote attackers to spoof servers via an arbitrary valid certificate.	curl	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-738
5374	CVE-2016-3718	MEDIUM	Medium	The (1) HTTP and (2) FTP coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to conduct server-side request forgery (SSRF) attacks via a crafted image.	imagemagick	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-607
5375	CVE-2016-3717	HIGH	Medium	The LABEL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to read arbitrary files via a crafted image.	imagemagick	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-648
5376	CVE-2016-3716	MEDIUM	Low	The MSL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to move arbitrary files via a crafted image.	imagemagick	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-573

	A	B	C	D	E	F	G	H	I	J	K	L	M
5377	CVE-2016-3715	MEDIUM	Medium	The EPHEMERAL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to delete arbitrary files via a crafted image.	imagemagick	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-623
5378	CVE-2016-3714	HIGH	High	The (1) EPHEMERAL, (2) HTTPS, (3) MVG, (4) MSL, (5) TEXT, (6) SHOW, (7) WIN, and (8) PLT coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to execute arbitrary code via shell metacharacters in a crafted image, aka ImageTragick.	imagemagick	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-665
5379	CVE-2016-3713	MEDIUM	High	The msr_mtrr_valid function in arch/x86/kvm/mtrr.c in the Linux kernel before 4.6.1 supports MSR 0x2f8, which allows guest OS users to read or write to the kvm_arch_vcpu data structure, and consequently obtain sensitive information or cause a denial of service (system crash), via a crafted ioctl call.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-926
5380	CVE-2016-3712	LOW	Medium	Integer overflow in the VGA module in QEMU allows local guest OS users to cause a denial of service (out-of-bounds read and QEMU process crash) by editing VGA registers in VBE mode.	qemu	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-621
5381	CVE-2016-3710	HIGH	High	The VGA module in QEMU improperly performs bounds checking on banked access to video memory, which allows local guest OS users to execute arbitrary code on the host by changing access modes after setting the bank register, aka the Dark Portal issue.	qemu	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-601
5382	CVE-2016-3707	MEDIUM	High	The icmp_check_sysrq function in net/ipv4/icmp.c in the kernel.org projects/rt patches for the Linux kernel, as used in the kernel-rt package before 3.10.0-327.22.1 in Red Hat Enterprise Linux for Real Time 7 and other products, allows remote attackers to execute SysRq commands via crafted ICMP Echo Request packets, as demonstrated by a brute-force attack to discover a cookie, or an attack that occurs after reading the local icmp_echo_sysrq file.	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-921
5383	CVE-2016-3706	MEDIUM	High	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in the GNU C Library (aka glibc or libc6) allows remote attackers to cause a denial of service (crash) via vectors involving hostent conversion. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4458.	glibc	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-839
5384	CVE-2016-3705	MEDIUM	High	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-690
5385	CVE-2016-3699	MEDIUM	High	The Linux kernel, as used in Red Hat Enterprise Linux 7.2 and Red Hat Enterprise MRG 2 and when booted with UEFI Secure Boot enabled, allows local users to bypass intended Secure Boot restrictions and execute untrusted code by appending ACPI tables to the initrd.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1739
5386	CVE-2016-3695	LOW	Medium	The einj_error_inject function in drivers/acpi/apei/einj.c in the Linux kernel allows local users to simulate hardware errors and consequently cause a denial of service by leveraging failure to disable APEI error injection through EINJ when securelevel is set.	linux	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3085
5387	CVE-2016-3689	MEDIUM	Medium	The ims_pcu_parse_cdc_data function in drivers/input/misc/ims-pcu.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (system crash) via a USB device without both a master and a slave interface.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-658
5388	CVE-2016-3672	MEDIUM	High	The arch_pick_mmap_layout function in arch/x86/mm/mmap.c in the Linux kernel through 4.5.2 does not properly randomize the legacy base address, which makes it easier for local users to defeat the intended restrictions on the ADDR_NO_RANDOMIZE flag, and bypass the ASLR protection mechanism for a setuid or setgid program, by disabling stack-consumption resource limits.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-527
5389	CVE-2016-3658	MEDIUM	High	The TIFFWriteDirectoryTagLongLong8Array function in tif_dirwrite.c in the tiffset tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving the ma variable.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1728
5390	CVE-2016-3634	MEDIUM	High	The tagCompare function in tif_dirinfo.c in the thumbnail tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to field_tag matching.	libtiff	Unchanged	Won't Fix	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1733
5391	CVE-2016-3633	MEDIUM	High	The setrow function in the thumbnail tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the src variable.	libtiff	Unchanged	Won't Fix	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1714
5392	CVE-2016-3632	MEDIUM	High	The _TIFFVGetField function in tif_dirinfo.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image.	libtiff	Unchanged	8.0.0.12	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1737
5393	CVE-2016-3631	MEDIUM	High	The (1) cpStrips and (2) cpTiles functions in the thumbnail tool in LibTIFF 4.0.6 and earlier allow remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the bytecounts[] array variable.	libtiff	Unchanged	Vulnerable	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1753
5394	CVE-2016-3630	MEDIUM	High	The binary delta decoder in Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a (1) clone, (2) push, or (3) pull command, related to (a) a list sizing rounding error and (b) short records.	mercurial	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-477
5395	CVE-2016-3627	MEDIUM	High	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-691

	A	B	C	D	E	F	G	H	I	J	K	L	M
5396	CVE-2016-3625	MEDIUM	Medium	tif_read.c in the tiff2bw tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TIFF image.	libtiff	Unchanged	Vulnerable	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1721
5397	CVE-2016-3624	MEDIUM	High	The cvtClump function in the rgb2ycbcr tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) by setting the -v option to -1.	libtiff	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1724
5398	CVE-2016-3623	MEDIUM	High	The rgb2ycbcr tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (divide-by-zero) by setting the (1) v or (2) h parameter to 0.	libtiff	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1748
5399	CVE-2016-3622	MEDIUM	Medium	The fpAcc function in tif_predict.c in the tiff2rgba tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted TIFF image.	libtiff	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1746
5400	CVE-2016-3621	MEDIUM	High	The LZWEncode function in tif_lzw.c in the bmp2tiff tool in LibTIFF 4.0.6 and earlier, when the -c lzw option is used, allows remote attackers to cause a denial of service (buffer over-read) via a crafted BMP image.	libtiff	Unchanged	Won't Fix	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1730
5401	CVE-2016-3620	MEDIUM	High	The ZIPEncode function in tif_zip.c in the bmp2tiff tool in LibTIFF 4.0.6 and earlier, when the -c zip option is used, allows remote attackers to cause a denial of service (buffer over-read) via a crafted BMP image.	libtiff	Unchanged	Won't Fix	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1710
5402	CVE-2016-3619	MEDIUM	Medium	The DumpModeEncode function in tif_dumpmode.c in the bmp2tiff tool in LibTIFF 4.0.6 and earlier, when the -c none option is used, allows remote attackers to cause a denial of service (buffer over-read) via a crafted BMP image.	libtiff	Unchanged	Won't Fix	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1717
5403	CVE-2016-3615	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: DML.	mysql	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1243
5404	CVE-2016-3614	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Security: Encryption.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1258
5405	CVE-2016-3610	HIGH	Critical	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Libraries, a different vulnerability than CVE-2016-3598.	jdk&jre	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1274
5406	CVE-2016-3606	MEDIUM	Critical	Unspecified vulnerability in Oracle Java SE 7u101 and 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot.	jdk&jre	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1264
5407	CVE-2016-3598	HIGH	Critical	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Libraries, a different vulnerability than CVE-2016-3610.	jdk&jre	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1241
5408	CVE-2016-3588	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote authenticated users to affect integrity and availability via vectors related to Server: InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1310
5409	CVE-2016-3587	HIGH	Critical	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot.	jdk&jre	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1276
5410	CVE-2016-3552	MEDIUM	High	Unspecified vulnerability in Oracle Java SE 8u92 allows local users to affect confidentiality, integrity, and availability via vectors related to Install.	jdk&jre	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1290
5411	CVE-2016-3550	MEDIUM	Medium	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality via vectors related to Hotspot.	jdk&jre	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1309
5412	CVE-2016-3521	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Types.	mysql	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1254
5413	CVE-2016-3518	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1240
5414	CVE-2016-3511	MEDIUM	High	Unspecified vulnerability in Oracle Java SE 7u101 and 8u92 allows local users to affect confidentiality, integrity, and availability via vectors related to Deployment.	jdk&jre	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1308
5415	CVE-2016-3508	MEDIUM	Medium	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; Java SE Embedded 8u91; and JRockit R28.3.10 allows remote attackers to affect availability via vectors related to JAXP, a different vulnerability than CVE-2016-3500.	jdk&jre	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1242
5416	CVE-2016-3503	MEDIUM	High	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92 allows local users to affect confidentiality, integrity, and availability via vectors related to Install.	jdk&jre	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1303
5417	CVE-2016-3501	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1283
5418	CVE-2016-3500	MEDIUM	Medium	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; Java SE Embedded 8u91; and JRockit R28.3.10 allows remote attackers to affect availability via vectors related to JAXP, a different vulnerability than CVE-2016-3508.	jdk&jre	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1313
5419	CVE-2016-3498	MEDIUM	Medium	Unspecified vulnerability in Oracle Java SE 7u101 and 8u92 allows remote attackers to affect availability via vectors related to JavaFX.	jdk&jre	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1246
5420	CVE-2016-3495	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2165
5421	CVE-2016-3492	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.	mysql	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2167

	A	B	C	D	E	F	G	H	I	J	K	L	M
5422	CVE-2016-3486	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: FTS.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1247
5423	CVE-2016-3485	LOW	Low	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; Java SE Embedded 8u91; and JRockit R28.3.10 allows local users to affect integrity via vectors related to Networking.	jdk&jre	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1259
5424	CVE-2016-3477	MEDIUM	High	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Parser.	mysql	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1293
5425	CVE-2016-3471	HIGH	High	Unspecified vulnerability in Oracle MySQL 5.5.45 and earlier and 5.6.26 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Option.	mysql	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1295
5426	CVE-2016-3459	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1282
5427	CVE-2016-3458	MEDIUM	Medium	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; and Java SE Embedded 8u91 allows remote attackers to affect integrity via vectors related to CORBA.	jdk&jre	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1249
5428	CVE-2016-3452	MEDIUM	Low	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.10 and earlier allows remote attackers to affect confidentiality via vectors related to Server: Security: Encryption.	mysql	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1250
5429	CVE-2016-3440	MEDIUM	High	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1275
5430	CVE-2016-3424	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1285
5431	CVE-2016-3191	HIGH	Critical	The compile_branch function in pcre_compile.c in PCRE 8.x before 8.39 and pcre2_compile.c in PCRE2 before 10.22 mishandles patterns containing an (*ACCEPT) substring in conjunction with nested parentheses, which allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow) via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, aka ZDI-CAN-3542.	pcre	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-399
5432	CVE-2016-3190	MEDIUM	High	The fill_xrgb32_lerp_opaque_spans function in cairo-image-compositor.c in cairo before 1.14.2 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a negative span length.	cairo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-493
5433	CVE-2016-3189	MEDIUM	Medium	Use-after-free vulnerability in bzip2recover in bzip2 1.0.6 allows remote attackers to cause a denial of service (crash) via a crafted bzip2 file, related to block ends set to before the start of the block.CWE-416: Use After Free	bzip2	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-957
5434	CVE-2016-3186	MEDIUM	Medium	Buffer overflow in the readextension function in gif2tiff.c in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (application crash) via a crafted GIF file.	libtiff	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-487
5435	CVE-2016-3185	MEDIUM	High	The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (type confusion and application crash) via crafted serialized _cookies data, related to the SoapClient::__call method in ext/soap/soap.c.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-704
5436	CVE-2016-3183	MEDIUM	Medium	The sycc422_t_rgb function in common/color.c in OpenJPEG before 2.1.1 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted jpeg2000 file.	openjpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3186
5437	CVE-2016-3177	HIGH	Critical	Multiple use-after-free and double-free vulnerabilities in gifcolor.c in GIFLIB 5.1.2 have unspecified impact and attack vectors.	giflib	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3183
5438	CVE-2016-3157	HIGH	High	The __switch_to function in arch/x86/kernel/process_64.c in the Linux kernel does not properly context-switch IOPL on 64-bit PV Xen guests, which allows guest OS users to gain privileges, cause a denial of service (guest OS crash), or obtain sensitive information by leveraging I/O port access.	linux	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-438
5439	CVE-2016-3156	LOW	Medium	The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which allows guest OS users to cause a denial of service (host OS networking outage) by arranging for a large number of IP addresses.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-634
5440	CVE-2016-3142	MEDIUM	High	The phar_parse_zipfile function in zip.c in the PHAR extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and application crash) by placing a PK\x05\x06 signature at an invalid location.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-437
5441	CVE-2016-3141	HIGH	Critical	Use-after-free vulnerability in wddx.c in the WDDX extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact by triggering a wddx_deserialize call on XML data containing a crafted var element.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-439
5442	CVE-2016-3140	MEDIUM	Medium	The digi_port_init function in drivers/usb/serial/digi_acceleport.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-664

	A	B	C	D	E	F	G	H	I	J	K	L	M
5443	CVE-2016-3139	MEDIUM	Medium	The wacom_probe function in drivers/input/tablet/wacom_sys.c in the Linux kernel before 3.17 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-616
5444	CVE-2016-3138	MEDIUM	Medium	The acm_probe function in drivers/usb/class/cdc-acm.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both a control and a data endpoint descriptor.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-595
5445	CVE-2016-3137	MEDIUM	Medium	drivers/usb/serial/cypress_m8.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both an interrupt-in and an interrupt-out endpoint descriptor, related to the cypress_generic_port_probe and cypress_open functions.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-625
5446	CVE-2016-3136	MEDIUM	Medium	The mct_u232_msr_to_state function in drivers/usb/serial/mct_u232.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device without two interrupt-in endpoint descriptors.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-560
5447	CVE-2016-3135	HIGH	High	Integer overflow in the xt_alloc_table_info function in net/netfilter/x_tables.c in the Linux kernel through 4.5.2 on 32-bit platforms allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.CWE-190: Integer Overflow or Wraparound	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-640
5448	CVE-2016-3134	HIGH	High	The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-659
5449	CVE-2016-3132	HIGH	Critical	Double free vulnerability in the SplDoublyLinkedList::offsetSet function in ext/spl/spl_dllist.c in PHP 7.x before 7.0.6 allows remote attackers to execute arbitrary code via a crafted index.	php	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1370
5450	CVE-2016-3125	MEDIUM	High	The mod_tls module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile directive, which might cause a weaker than intended Diffie-Hellman (DH) key to be used and consequently allow attackers to have unspecified impact via unknown vectors.	proftpd	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-435
5451	CVE-2016-3120	MEDIUM	Medium	The validate_as_request function in kdc_util.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.13.6 and 1.4.x before 1.14.3, when restrict_anonymous_to_tgt is enabled, uses an incorrect client data structure, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via an S4U2Self request.	krb5	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1359
5452	CVE-2016-3119	LOW	Medium	The process_db_args function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in kadmind in MIT Kerberos 5 (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted request to modify a principal.CWE-476: NULL Pointer Dereference	krb5	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-392
5453	CVE-2016-3116	MEDIUM	Medium	CRLF injection vulnerability in Dropbear SSH before 2016.72 allows remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data.CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection')	dropbear	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3067
5454	CVE-2016-3115	MEDIUM	Medium	Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection')	openssh	Unchanged	8.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-407
5455	CVE-2016-3105	MEDIUM	High	The convert extension in Mercurial before 3.8 might allow context-dependent attackers to execute arbitrary code via a crafted git repository name.	mercurial	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-633
5456	CVE-2016-3104	MEDIUM	High	mongod in MongoDB 2.6, when using 2.4-style users, and 2.4 allow remote attackers to cause a denial of service (memory consumption and process termination) by leveraging in-memory database representation when authenticating against a non-existent database.	mongodb	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4011
5457	CVE-2016-3078	HIGH	Critical	Multiple integer overflows in php_zip.c in the zip extension in PHP before 7.0.6 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted call to (1) getFromIndex or (2) getFromName in the ZipArchive class.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1371

	A	B	C	D	E	F	G	H	I	J	K	L	M
5458	CVE-2016-3075	MEDIUM	High	Stack-based buffer overflow in the nss_dns implementation of the getnetbyname function in GNU C Library (aka glibc) before 2.24 allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a long name.	glibc	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-837
5459	CVE-2016-3070	MEDIUM	High	A security flaw was found in the Linux kernel that an attempt to move page mapped by AIO ring buffer to the other node triggers NULL pointer dereference at trace_writeback_dirty_page(), because aio_fs_backing_dev_info.dev is 0.	linux	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-943
5460	CVE-2016-3069	MEDIUM	High	Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a crafted name when converting a Git repository.	mercurial	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-509
5461	CVE-2016-3068	MEDIUM	High	Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a crafted git ext:: URL when cloning a subrepository.	mercurial	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-482
5462	CVE-2016-3065	HIGH	Critical	The (1) brin_page_type and (2) brin_metapage_info functions in the pageinspect extension in PostgreSQL before 9.5.x before 9.5.2 allows attackers to bypass intended access restrictions and consequently obtain sensitive server memory information or cause a denial of service (server crash) via a crafted bytea value in a BRIN index page.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-436
5463	CVE-2016-3062	MEDIUM	High	The mov_read_dref function in libavformat/mov.c in Libav before 11.7 and FFmpeg before 0.11 allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via the entries value in a dref box in an MP4 file.	libav	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-920
5464	CVE-2016-2858	LOW	Medium	QEMU, when built with the Pseudo Random Number Generator (PRNG) back-end support, allows guest OS users to cause a denial of service (process crash) via an entropy request, which triggers arbitrary stack based allocation and memory corruption.	qemu	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-434
5465	CVE-2016-2857	LOW	Medium	The net_checksum_calculate function in net/checksum.c in QEMU allows guest OS users to cause a denial of service (out-of-bounds heap read and crash) via the payload length in a crafted packet.	qemu	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-431
5466	CVE-2016-2854	MEDIUM	High	The aufs module for the Linux kernel 3.x and 4.x does not properly maintain POSIX ACL xattr data, which allows local users to gain privileges by leveraging a group-writable setgid directory.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-568
5467	CVE-2016-2853	MEDIUM	High	The aufs module for the Linux kernel 3.x and 4.x does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an aufs filesystem on top of a FUSE filesystem, and then executing a crafted setuid program.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-672
5468	CVE-2016-2851	HIGH	Critical	Integer overflow in proto.c in libotr before 4.1.1 on 64-bit platforms allows remote attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code via a series of large OTR messages, which triggers a heap-based buffer overflow.	libotr	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-429
5469	CVE-2016-2848	MEDIUM	High	ISC BIND 9.1.0 through 9.8.4-P2 and 9.9.0 through 9.9.2-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via malformed options data in an OPT resource record.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1832
5470	CVE-2016-2847	MEDIUM	Medium	fs/pipe.c in the Linux kernel before 4.5 does not limit the amount of unread data in pipes, which allows local users to cause a denial of service (memory consumption) by creating many pipes with non-default sizes.	linux	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-641
5471	CVE-2016-2844	HIGH	High	WebKit/Source/core/layout/LayoutBlock.cpp in Blink, as used in Google Chrome before 49.0.2623.75, does not properly determine when anonymous block wrappers may exist, which allows remote attackers to cause a denial of service (incorrect cast and assertion failure) or possibly have unspecified other impact via crafted JavaScript code.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-355
5472	CVE-2016-2842	HIGH	Critical	The doapr_outch function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not verify that a certain memory allocation succeeds, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-0799.	openssl	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-338
5473	CVE-2016-2834	HIGH	High	Mozilla Network Security Services (NSS) before 3.23, as used in Mozilla Firefox before 47.0, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.	nss	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-919
5474	CVE-2016-2782	MEDIUM	Medium	The treo_attach function in drivers/usb/serial/visor.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by inserting a USB device that lacks a (1) bulk-in or (2) interrupt-in endpoint.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-597
5475	CVE-2016-2781	LOW	Medium	chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.	coreutils	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-3233
5476	CVE-2016-2779	HIGH	High	runuser in util-linux allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.	util-linux	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3317
5477	CVE-2016-2776	HIGH	High	buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.	bind	Unchanged	8.0.0.11	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1666

	A	B	C	D	E	F	G	H	I	J	K	L	M
5478	CVE-2016-2775	MEDIUM	Medium	ISC BIND 9.x before 9.9.9-P2, 9.10.x before 9.10.4-P2, and 9.11.x before 9.11.0b2, when lwresd or the named lwres option is enabled, allows remote attackers to cause a denial of service (daemon crash) via a long request that uses the lightweight resolver protocol.	bind	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1284
5479	CVE-2016-2774	HIGH	Medium	ISC DHCP 4.1.x before 4.1-ESV-R13 and 4.2.x and 4.3.x before 4.3.4 does not restrict the number of concurrent TCP sessions, which allows remote attackers to cause a denial of service (INSIST assertion failure or request-processing outage) by establishing many sessions.	dhcp	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-345
5480	CVE-2016-2572	MEDIUM	High	http.cc in Squid 4.x before 4.0.7 relies on the HTTP status code after a response-parsing failure, which allows remote HTTP servers to cause a denial of service (assertion failure and daemon exit) via a malformed response.	squid	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-363
5481	CVE-2016-2571	MEDIUM	High	http.cc in Squid 3.x before 3.5.15 and 4.x before 4.0.7 proceeds with the storage of certain data after a response-parsing failure, which allows remote HTTP servers to cause a denial of service (assertion failure and daemon exit) via a malformed response.	squid	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-372
5482	CVE-2016-2570	MEDIUM	High	The Edge Side Includes (ESI) parser in Squid 3.x before 3.5.15 and 4.x before 4.0.7 does not check buffer limits during XML parsing, which allows remote HTTP servers to cause a denial of service (assertion failure and daemon exit) via a crafted XML document, related to esi/CustomParser.cc and esi/CustomParser.h.	squid	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-344
5483	CVE-2016-2569	MEDIUM	High	Squid 3.x before 3.5.15 and 4.x before 4.0.7 does not properly append data to String objects, which allows remote servers to cause a denial of service (assertion failure and daemon exit) via a long string, as demonstrated by a crafted HTTP Vary header.	squid	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-357
5484	CVE-2016-2562	MEDIUM	Medium	The checkHTTP function in libraries/Config.class.php in phpMyAdmin 4.5.x before 4.5.5.1 does not verify X.509 certificates from api.github.com SSL servers, which allows man-in-the-middle attackers to spoof these servers and obtain sensitive information via a crafted certificate.	phpmyadmin	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-356
5485	CVE-2016-2561	LOW	Medium	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.4.x before 4.4.15.5 and 4.5.x before 4.5.5.1 allow remote authenticated users to inject arbitrary web script or HTML via (1) normalization.php or (2) js/normalization.js in the database normalization page, (3) templates/database/structure/sortable_header.phtml in the database structure page, or (4) the pos parameter to db_central_columns.php in the central columns page.	phpmyadmin	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-369
5486	CVE-2016-2560	MEDIUM	Medium	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.15, 4.4.x before 4.4.15.5, and 4.5.x before 4.5.5.1 allow remote attackers to inject arbitrary web script or HTML via (1) a crafted Host HTTP header, related to libraries/Config.class.php; (2) crafted JSON data, related to file_echo.php; (3) a crafted SQL query, related to js/functions.js; (4) the initial parameter to libraries/server_privileges.lib.php in the user accounts page; or (5) the it parameter to libraries/controllers/TableSearchController.class.php in the zoom search page.	phpmyadmin	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-346
5487	CVE-2016-2559	LOW	Medium	Cross-site scripting (XSS) vulnerability in the format function in libraries/sql-parser/src/Utils/Error.php in the SQL parser in phpMyAdmin 4.5.x before 4.5.5.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted query.	phpmyadmin	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-362
5488	CVE-2016-2554	HIGH	Critical	Stack-based buffer overflow in ext/phar/tar.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TAR archive.	php	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-708
5489	CVE-2016-2550	MEDIUM	Medium	The Linux kernel before 4.5 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by leveraging incorrect tracking of descriptor ownership and sending each descriptor over a UNIX socket before closing it. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-4312.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-668
5490	CVE-2016-2549	LOW	Medium	sound/core/hrtimer.c in the Linux kernel before 4.4.1 does not prevent recursive callback access, which allows local users to cause a denial of service (deadlock) via a crafted ioctl call.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-562
5491	CVE-2016-2548	MEDIUM	Medium	sound/core/timer.c in the Linux kernel before 4.4.1 retains certain linked lists after a close or stop action, which allows local users to cause a denial of service (system crash) via a crafted ioctl call, related to the (1) snd_timer_close and (2) _snd_timer_stop functions.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-642
5492	CVE-2016-2547	MEDIUM	Medium	sound/core/timer.c in the Linux kernel before 4.4.1 employs a locking approach that does not consider slave timer instances, which allows local users to cause a denial of service (race condition, use-after-free, and system crash) via a crafted ioctl call.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-594
5493	CVE-2016-2546	MEDIUM	Medium	sound/core/timer.c in the Linux kernel before 4.4.1 uses an incorrect type of mutex, which allows local users to cause a denial of service (race condition, use-after-free, and system crash) via a crafted ioctl call.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-662
5494	CVE-2016-2545	MEDIUM	Medium	The snd_timer_interrupt function in sound/core/timer.c in the Linux kernel before 4.4.1 does not properly maintain a certain linked list, which allows local users to cause a denial of service (race condition and system crash) via a crafted ioctl call.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-611
5495	CVE-2016-2544	MEDIUM	Medium	Race condition in the queue_delete function in sound/core/seq/seq_queue.c in the Linux kernel before 4.4.1 allows local users to cause a denial of service (use-after-free and system crash) by making an ioctl call at a certain time.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-558

	A	B	C	D	E	F	G	H	I	J	K	L	M
5496	CVE-2016-2543	MEDIUM	Medium	The snd_seq_ioctl_remove_events function in sound/core/seq/seq_clientmgr.c in the Linux kernel before 4.4.1 does not verify FIFO assignment before proceeding with FIFO clearing, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted ioctl call.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-636
5497	CVE-2016-2538	LOW	High	Multiple integer overflows in the USB Net device emulator (hw/usb/dev-network.c) in QEMU before 2.5.1 allow local guest OS administrators to cause a denial of service (QEMU process crash) or obtain sensitive host memory information via a remote NDIS control message packet that is mishandled in the (1) rndis_query_response, (2) rndis_set_response, or (3) usb_net_handle_dataout function.	qemu	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-935
5498	CVE-2016-2533	MEDIUM	Medium	Buffer overflow in the ImagingPcdDecode function in PcdDecode.c in Pillow before 3.1.1 and Python Imaging Library (PIL) 1.1.7 and earlier allows remote attackers to cause a denial of service (crash) via a crafted PhotoCD file.	python-imaging	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-473
5499	CVE-2016-2532	MEDIUM	Medium	The dissect_llrp_parameters function in epan/dissectors/packet-llrp.c in the LLRP dissector in Wireshark 1.12.x before 1.12.10 and 2.0.x before 2.0.2 does not limit the recursion depth, which allows remote attackers to cause a denial of service (memory consumption or application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-349
5500	CVE-2016-2531	MEDIUM	Medium	Off-by-one error in epan/dissectors/packet-rsl.c in the RSL dissector in Wireshark 1.12.x before 1.12.10 and 2.0.x before 2.0.2 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet that triggers a 0xff tag value, a different vulnerability than CVE-2016-2530.	wireshark	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-360
5501	CVE-2016-2530	MEDIUM	Medium	The dissct_rsl_ipaccess_msg function in epan/dissectors/packet-rsl.c in the RSL dissector in Wireshark 1.12.x before 1.12.10 and 2.0.x before 2.0.2 mishandles the case of an unrecognized TLV type, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet, a different vulnerability than CVE-2016-2531.	wireshark	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-354
5502	CVE-2016-2529	MEDIUM	Medium	The iseries_check_file_type function in wiretap/iseries.c in the iSeries file parser in Wireshark 2.0.x before 2.0.2 does not consider that a line may lack the OBJECT PROTOCOL substring, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted file.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-343
5503	CVE-2016-2528	MEDIUM	Medium	The dissect_nhdr_extopt function in epan/dissectors/packet-lbmc.c in the LBMC dissector in Wireshark 2.0.x before 2.0.2 does not validate length values, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-368
5504	CVE-2016-2527	MEDIUM	Medium	wiretap/nettrace_3gpp_32_423.c in the 3GPP TS 32.423 Trace file parser in Wireshark 2.0.x before 2.0.2 does not ensure that a '\0' character is present at the end of certain strings, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted file.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-348
5505	CVE-2016-2526	MEDIUM	Medium	epan/dissectors/packet-hiqnet.c in the HiQnet dissector in Wireshark 2.0.x before 2.0.2 does not validate the data type, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-347
5506	CVE-2016-2525	MEDIUM	Medium	epan/dissectors/packet-http2.c in the HTTP/2 dissector in Wireshark 2.0.x before 2.0.2 does not limit the amount of header data, which allows remote attackers to cause a denial of service (memory consumption or application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-359
5507	CVE-2016-2524	MEDIUM	Medium	epan/dissectors/packet-x509af.c in the X.509AF dissector in Wireshark 2.0.x before 2.0.2 mishandles the algorithm ID, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-351
5508	CVE-2016-2523	HIGH	Medium	The dnp3_al_process_object function in epan/dissectors/packet-dnp.c in the DNP3 dissector in Wireshark 1.12.x before 1.12.10 and 2.0.x before 2.0.2 allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	wireshark	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-350
5509	CVE-2016-2522	MEDIUM	Medium	The dissect_ber_constrained_bitstring function in epan/dissectors/packet-ber.c in the ASN.1 BER dissector in Wireshark 2.0.x before 2.0.2 does not verify that a certain length is nonzero, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-364
5510	CVE-2016-2521	HIGH	High	Untrusted search path vulnerability in the WiresharkApplication class in ui/qt/wireshark_application.cpp in Wireshark 1.12.x before 1.12.10 and 2.0.x before 2.0.2 on Windows allows local users to gain privileges via a Trojan horse riched20.dll.dll file in the current working directory, related to use of QLibrary.	wireshark	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-361

	A	B	C	D	E	F	G	H	I	J	K	L	M
5511	CVE-2016-2519	MEDIUM	Medium	ntpq and ntpdc can be used to store and retrieve information in ntpd. It is possible to store a data value that is larger than the size of the buffer that the ctl_getitem() function of ntpd uses to zreport the return value. If the length of the requested data value returned by ctl_getitem() is too large, the value NULL is returned instead. There are 2 cases where the return value from ctl_getitem() was not directly checked to make sure it's not NULL, but there are subsequent INSIST() checks that make sure the return value is not NULL. There are no data values ordinarily stored in ntpd that would exceed this buffer length. But if one has permission to store values and one stores a value that is "too large", then ntpd will abort if an attempt is made to read that oversized value.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-825
5512	CVE-2016-2518	MEDIUM	Medium	Using a crafted packet to create a peer association with hmode > 7 causes the MATCH_ASSOC() lookup to make an out-of-bounds reference.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-850
5513	CVE-2016-2517	MEDIUM	Medium	If ntpd was expressly configured to allow for remote configuration, a malicious user who knows the controlkey for ntpq or the requestkey for ntpdc (if mode7 is expressly enabled) can create a session with ntpd and then send a crafted packet to ntpd that will change the value of the trustedkey, controlkey, or requestkey to a value that will prevent any subsequent authentication with ntpd until ntpd is restarted.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-817
5514	CVE-2016-2516	HIGH	Medium	If ntpd was expressly configured to allow for remote configuration, a malicious user who knows the controlkey for ntpq or the requestkey for ntpdc (if mode7 is expressly enabled) can create a session with ntpd and if an existing association is unconfigured using the same IP twice on the unconfig directive line, ntpd will abort.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-821
5515	CVE-2016-2392	LOW	Medium	The is_rndis function in the USB Net device emulator (hw/usb/dev-network.c) in QEMU before 2.5.1 does not properly validate USB configuration descriptor objects, which allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors involving a remote NDIS control message packet.CWE-476: NULL Pointer Dereference	qemu	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-928
5516	CVE-2016-2391	LOW	Medium	The ohci_bus_start function in the USB OHCI emulation support (hw/usb/hcd-ohci.c) in QEMU allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors related to multiple eof_timers.CWE-476: NULL Pointer Dereference	qemu	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-924
5517	CVE-2016-2390	MEDIUM	Medium	The FwdState::connectedToPeer method in FwdState.cc in Squid before 3.5.14 and 4.0.x before 4.0.6 does not properly handle SSL handshake errors when built with the --with-openssl option, which allows remote attackers to cause a denial of service (application crash) via a plaintext HTTP message.	squid	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-504
5518	CVE-2016-2384	MEDIUM	Medium	Double free vulnerability in the snd_usbmidi_create function in sound/usb/midi.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly have unspecified other impact via vectors involving an invalid USB descriptor.CWE-415: Double Free	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-610
5519	CVE-2016-2383	LOW	Medium	The adjust_branches function in kernel/bpf/verifier.c in the Linux kernel before 4.5 does not consider the delta in the backward-jump case, which allows local users to obtain sensitive information from kernel memory by creating a packet filter and then loading crafted BPF instructions.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-559
5520	CVE-2016-2381	MEDIUM	Medium	Perl might allow context-dependent attackers to bypass the taint protection mechanism in a child process via duplicate environment variables in envp.	perl	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-432
5521	CVE-2016-2380	MEDIUM	Low	An information leak exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent to the server could potentially result in an out-of-bounds read. A user could be convinced to enter a particular string which would then get converted incorrectly and could lead to a potential out-of-bounds read.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3007
5522	CVE-2016-2378	MEDIUM	High	A buffer overflow vulnerability exists in the handling of the MXIT protocol Pidgin. Specially crafted data sent via the server could potentially result in a buffer overflow, potentially resulting in memory corruption. A malicious server or an unfiltered malicious user can send negative length values to trigger this vulnerability.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3008
5523	CVE-2016-2377	MEDIUM	High	A buffer overflow vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent by the server could potentially result in an out-of-bounds write of one byte. A malicious server can send a negative content-length in response to a HTTP request triggering the vulnerability.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2987
5524	CVE-2016-2376	MEDIUM	High	A buffer overflow vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent from the server could potentially result in arbitrary code execution. A malicious server or an attacker who intercepts the network traffic can send an invalid size for a packet which will trigger a buffer overflow.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3001
5525	CVE-2016-2375	MEDIUM	Medium	An exploitable out-of-bounds read exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT contact information sent from the server can result in memory disclosure.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2955

	A	B	C	D	E	F	G	H	I	J	K	L	M
5526	CVE-2016-2374	MEDIUM	High	An exploitable memory corruption vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT MultiMX message sent via the server can result in an out-of-bounds write leading to memory disclosure and code execution.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2960
5527	CVE-2016-2373	MEDIUM	Medium	A denial of service vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in an out-of-bounds read. A malicious server or user can send an invalid mood to trigger this vulnerability.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2985
5528	CVE-2016-2372	MEDIUM	Medium	An information leak exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in an out-of-bounds read. A malicious user, server, or man-in-the-middle attacker can send an invalid size for a file transfer which will trigger an out-of-bounds read vulnerability. This could result in a denial of service or copy data from memory to the file, resulting in an information leak if the file is sent to another user.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3002
5529	CVE-2016-2371	MEDIUM	High	An out-of-bounds write vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could cause memory corruption resulting in code execution.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2958
5530	CVE-2016-2370	MEDIUM	Medium	A denial of service vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent from the server could potentially result in an out-of-bounds read. A malicious server or man-in-the-middle attacker can send invalid data to trigger this vulnerability.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2983
5531	CVE-2016-2369	MEDIUM	Medium	A NULL pointer dereference vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in a denial of service vulnerability. A malicious server can send a packet starting with a NULL byte triggering the vulnerability.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3004
5532	CVE-2016-2368	HIGH	High	Multiple memory corruption vulnerabilities exist in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could result in multiple buffer overflows, potentially resulting in code execution or memory disclosure.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2954
5533	CVE-2016-2367	LOW	Medium	An information leak exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in an out-of-bounds read. A malicious user, server, or man-in-the-middle can send an invalid size for an avatar which will trigger an out-of-bounds read vulnerability. This could result in a denial of service or copy data from memory to the file, resulting in an information leak if the avatar is sent to another user.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3003
5534	CVE-2016-2366	MEDIUM	Medium	A denial of service vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in an out-of-bounds read. A malicious server or an attacker who intercepts the network traffic can send invalid data to trigger this vulnerability and cause a crash.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2972
5535	CVE-2016-2365	MEDIUM	Medium	A denial of service vulnerability exists in the handling of the MXIT protocol in Pidgin. Specially crafted MXIT data sent via the server could potentially result in a null pointer dereference. A malicious server or an attacker who intercepts the network traffic can send invalid data to trigger this vulnerability and cause a crash.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3000
5536	CVE-2016-2342	HIGH	High	The bgp_nlri_parse_vpnv4 function in bgp_mplsvpn.c in the VPNv4 NLRI parser in bgpd in Quagga before 1.0.20160309, when a certain VPNv4 configuration is used, relies on a Labeled-VPN SAFI routes-data length field during a data copy, which allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow) via a crafted packet.	quagga	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-403
5537	CVE-2016-2339	HIGH	Critical	An exploitable heap overflow vulnerability exists in the Fiddle::Function.new initialize function functionality of Ruby. In Fiddle::Function.new initialize heap buffer arg_types allocation is made based on args array length. Specially constructed object passed as element of args array can increase this array size after mentioned allocation and cause heap overflow.	ruby	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2953
5538	CVE-2016-2337	HIGH	Critical	Type confusion exists in _cancel_eval Ruby's TclTkIp class method. Attacker passing different type of object than String as retval argument can cause arbitrary code execution.CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')	ruby&tcltk	Unchanged	8.0.0.14	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2991
5539	CVE-2016-2330	MEDIUM	High	libavcodec/gif.c in FFmpeg before 2.8.6 does not properly calculate a buffer size, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via a crafted .tga file, related to the gif_image_write_image, gif_encode_init, and gif_encode_close functions.	gst-ffmpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-221
5540	CVE-2016-2329	MEDIUM	High	libavcodec/tiff.c in FFmpeg before 2.8.6 does not properly validate RowsPerStrip values and YCbCr chrominance subsampling factors, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via a crafted TIFF file, related to the tiff_decode_tag and decode_frame functions.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-251
5541	CVE-2016-2328	MEDIUM	High	libswscale/swscale_unscaled.c in FFmpeg before 2.8.6 does not validate certain height values, which allows remote attackers to cause a denial of service (out-of-bounds array read access) or possibly have unspecified other impact via a crafted .cine file, related to the bayer_to_rgb24_wrapper and bayer_to_yv12_wrapper functions.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-238

	A	B	C	D	E	F	G	H	I	J	K	L	M
5542	CVE-2016-2327	MEDIUM	High	libavcodec/pngenc.c in FFmpeg before 2.8.5 uses incorrect line sizes in certain row calculations, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via a crafted .avi file, related to the apng_encode_frame and encode_apng functions.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-255
5543	CVE-2016-2326	MEDIUM	High	Integer overflow in the asf_write_packet function in libavformat/asfenc.c in FFmpeg before 2.8.5 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PTS (aka presentation timestamp) value in a .mov file.	gst-ffmpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-225
5544	CVE-2016-2324	HIGH	Critical	An integer truncation flaw and an integer overflow flaw, both leading to a heap-based buffer overflow, were found in the way Git processed certain path information. A remote attacker could create a specially crafted Git repository that would cause a Git client or server to crash or, possibly, execute arbitrary code.	git	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-411
5545	CVE-2016-2315	HIGH	Critical	An integer truncation flaw and an integer overflow flaw, both leading to a heap-based buffer overflow, were found in the way Git processed certain path information. A remote attacker could create a specially crafted Git repository that would cause a Git client or server to crash or, possibly, execute arbitrary code.	git	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-412
5546	CVE-2016-2226	MEDIUM	High	A vulnerability was found in gcc. Specifically, it revolves around demangling while analysing the untrusted binaries. A particularly malicious attacker could craft an executable that executes when *analysed* by objdump, nm or gdb, or any other libbfd / libiberty - based forensics tool (if the demangling option is switched on).	gcc	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-680
5547	CVE-2016-2225	MEDIUM	High	The other problem is that a crafted packet will make the parser terminate early. The buffer is never initialized and is later passed to Strdup()	uclibc	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-316
5548	CVE-2016-2224	MEDIUM	High	A denial of service while parsing compressed items. An attacker can make the application end up in an infinit loop.	uclibc	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-302
5549	CVE-2016-2217	MEDIUM	Medium	It was found that in the OpenSSL address implementation the hard coded 1024 bit DH p parameter was not prime. The effective cryptographic strength of a key exchange using these parameters was weaker than the one one could get by using a prime p, making easier for eavesdropper to recover the shared secret from a key exchange that uses them.	socat	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-289
5550	CVE-2016-2213	MEDIUM	Medium	The jpeg2000_decode_tile function in libavcodec/jpeg2000dec.c in FFmpeg before 2.8.6 allows remote attackers to cause a denial of service (out-of-bounds array read access) via crafted JPEG 2000 data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-224
5551	CVE-2016-2198	LOW	Medium	Qemu emulator built with the USB EHCI emulation support is vulnerable to a null pointer dereference flaw. It could occur when an application attempts to write to EHCI capabilities registers.	qemu	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-298
5552	CVE-2016-2197	LOW	Medium	Qemu emulator built with an IDE AHCI emulation support is vulnerable to a null pointer dereference flaw. It occurs while unmapping the Frame Information Structure(FIS) & Command List Block(CLB) entries.	qemu	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-307
5553	CVE-2016-2193	MEDIUM	High	PostgreSQL before 9.5.x before 9.5.2 does not properly maintain row-security status in cached plans, which might allow attackers to bypass intended access restrictions by leveraging a session that performs queries as more than one role.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-428
5554	CVE-2016-2188	MEDIUM	Medium	The iowarrior_probe function in drivers/usb/misc/iowarrior.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-583
5555	CVE-2016-2187	MEDIUM	Medium	The gtco_probe function in drivers/input/tablet/gtco.c in the Linux kernel through 4.5.2 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-632
5556	CVE-2016-2186	MEDIUM	Medium	The powermate_probe function in drivers/input/misc/powermate.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-613
5557	CVE-2016-2185	MEDIUM	Medium	The ati_remote2_probe function in drivers/input/misc/ati_remote2.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-669
5558	CVE-2016-2184	MEDIUM	Medium	The create_fixed_stream_quirk function in sound/usb/quirks.c in the snd-usb-audio driver in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference or double free, and system crash) via a crafted endpoints value in a USB device descriptor.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-638

	A	B	C	D	E	F	G	H	I	J	K	L	M
5559	CVE-2016-2183	MEDIUM	Medium	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a Sweet32 attack.	openssl	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1525
5560	CVE-2016-2182	HIGH	Critical	An out-of-bounds write vulnerability was found to be caused by not checking errors in BN_bn2dec(). If an oversize BIGNUM is presented to BN_bn2dec() it can cause BN_div_word() to fail and not reduce the value of 't' resulting in OOB writes to the bn_data buffer and eventually crashing.	openssl	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1505
5561	CVE-2016-2181	MEDIUM	High	It was found that when doing handshake/ renegotiation, it's possible to bypass DTLS replay protection by sending a record for the next epoch (which does not have to decrypt or have a valid MAC), with a very large sequence number. This means the right hand edge of the window is moved very far to the right, and all subsequent legitimate packets are dropped causing a denial of service.	openssl	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1523
5562	CVE-2016-2180	MEDIUM	High	The TS_OBJ_print_bio function in crypto/ ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the openssl ts command.	openssl	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1377
5563	CVE-2016-2179	MEDIUM	High	It was found that current mechanism of queuing the future messages, i.e. messages having greater sequence numbers that are to be processed later, is prone to DoS attack by memory exhaustion, when attacker can fill up the queue with lots of large messages that are never going to be used. Only up to 10 messages in the future can be buffered and queue gets cleared when the connection is closed, thus attacker can exploit this only with opening many simultaneous connections.	openssl	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1522
5564	CVE-2016-2178	LOW	Medium	The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.	openssl	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-854
5565	CVE-2016-2177	HIGH	Critical	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.CWE-190: Integer Overflow or Wraparound	openssl	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-855
5566	CVE-2016-2176	MEDIUM	High	The X509_NAME_oneline function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.	openssl	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-554
5567	CVE-2016-2168	MEDIUM	Medium	The req_check_access function in the mod_authz_svn module in the httpd server in Apache Subversion before 1.8.16 and 1.9.x before 1.9.4 allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via a crafted header in a (1) MOVE or (2) COPY request, involving an authorization check.CWE-476: NULL Pointer Dereference	subversion	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-571
5568	CVE-2016-2167	MEDIUM	Medium	The canonicalize_username function in svnserve/cyrus_auth.c in Apache Subversion before 1.8.16 and 1.9.x before 1.9.4, when Cyrus SASL authentication is used, allows remote attackers to authenticate and bypass intended access restrictions via a realm string that is a prefix of an expected repository realm string.	subversion	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-590
5569	CVE-2016-2161	MEDIUM	High	It was discovered that the mod_auth_digest module of httpd did not properly check for memory allocation failures. A remote attacker could use this flaw to cause httpd child processes to repeatedly crash if the server used HTTP digest authentication, could use this flaw to decrypt and modify session data using a padding oracle attack.	apache	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3986
5570	CVE-2016-2148	HIGH	Critical	A heap based buffer overflow was discovered in udhcpc when parsing IPv6 Rapid Deployment DHCP option. An attacker could send a maliciously crafted packet as an answer to a DHCP request, to overwrite the heap, resulting in crash or remote code execution.	busybox	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-676
5571	CVE-2016-2147	MEDIUM	High	An out of bound write was discovered in udhcpc when parsing the Domain Search option. An attacker could send a maliciously crafted packet answering a DHCP request triggering a denial of service on the client. request, to overwrite the heap, resulting in crash or remote code execution.	busybox	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-677
5572	CVE-2016-2143	MEDIUM	High	The fork implementation in the Linux kernel before 4.5 on s390 platforms mishandles the case of four page-table levels, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted application, related to arch/s390/include/asm/mmu_context.h and arch/s390/include/asm/pgalloc.h.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-582

	A	B	C	D	E	F	G	H	I	J	K	L	M
5573	CVE-2016-2126	Medium	Medium	Samba version 4.0.0 up to 4.5.2 is vulnerable to privilege elevation due to incorrect handling of the PAC (Privilege Attribute Certificate) checksum. A remote, authenticated, attacker can cause the winbindd process to crash using a legitimate Kerberos ticket. A local service with access to the winbindd privileged pipe can cause winbindd to cache elevated access permissions.	samba	Unchanged	8.0.0.21	9.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4998
5574	CVE-2016-2125	LOW	MEDIUM	Samba client code always requests a forwardable ticket when using Kerberos authentication. This means the target server, which must be in the current or trusted domain/realm, is given a valid general purpose Kerberos "Ticket Granting Ticket" (TGT), which can be used to fully impersonate the authenticated user or service.	samba	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5143
5575	CVE-2016-2123	MEDIUM	HIGH	Authenicated users can supply malicious dnsRecord attributes on DNS objects and trigger a controlled memory corruption.	samba	Unchanged	8.0.0.22	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5148
5576	CVE-2016-2119	MEDIUM	High	libcli/smb/smbXcli_base.c in Samba 4.x before 4.2.14, 4.3.x before 4.3.11, and 4.4.x before 4.4.5 allows man-in-the-middle attackers to bypass a client-signing protection mechanism, and consequently spoof SMB2 and SMB3 servers, via the (1) SMB2_SESSION_FLAG_IS_GUEST or (2) SMB2_SESSION_FLAG_IS_NULL flag.	samba	Unchanged	8.0.0.10	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1131
5577	CVE-2016-2118	MEDIUM	High	The MS-SAMR and MS-LSAD protocol implementations in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 mishandle DCERPC connections, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka BADLOCK.	samba	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-426
5578	CVE-2016-2117	MEDIUM	High	The atl2_probe function in drivers/net/ethernet/atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly enables scatter/gather I/O, which allows remote attackers to obtain sensitive information from kernel memory by reading packet data.	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-577
5579	CVE-2016-2116	MEDIUM	Medium	Memory leak in the jas_iccprof_createfrombuf function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (memory consumption) via a crafted ICC color profile in a JPEG 2000 image file. Crafted ICC color profile in a JPEG 2000 image file, a different vulnerability than CVE-2014-8137.	jasper	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-450
5580	CVE-2016-2115	MEDIUM	Medium	Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not require SMB signing within a DCERPC session over ncacn_np, which allows man-in-the-middle attackers to spoof SMB clients by modifying the client-server data stream.	samba	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-516
5581	CVE-2016-2114	MEDIUM	Medium	The SMB1 protocol implementation in Samba 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not recognize the server signing = mandatory setting, which allows man-in-the-middle attackers to spoof SMB servers by modifying the client-server data stream.	samba	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-507
5582	CVE-2016-2113	MEDIUM	High	Samba 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not verify X.509 certificates from TLS servers, which allows man-in-the-middle attackers to spoof LDAPS and HTTPS servers and obtain sensitive information via a crafted certificate.	samba	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-514
5583	CVE-2016-2112	MEDIUM	Medium	The bundled LDAP client library in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not recognize the client ldap sasl wrapping setting, which allows man-in-the-middle attackers to perform LDAP protocol-downgrade attacks by modifying the client-server data stream.	samba	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-491
5584	CVE-2016-2111	MEDIUM	Medium	The NETLOGON service in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2, when a domain controller is configured, allows remote attackers to spoof the computer name of a secure channel's endpoint, and obtain sensitive session information, by running a crafted application and leveraging the ability to sniff network traffic, a related issue to CVE-2015-0005.	samba	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-466
5585	CVE-2016-2110	MEDIUM	Medium	The NTLMSSP authentication implementation in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 allows man-in-the-middle attackers to perform protocol-downgrade attacks by modifying the client-server data stream to remove application-layer flags or encryption settings, as demonstrated by clearing the NTLMSSP_NEGOTIATE_SEAL or NTLMSSP_NEGOTIATE_SIGN option to disrupt LDAP security.	samba	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-506
5586	CVE-2016-2109	HIGH	High	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.	openssl	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-551
5587	CVE-2016-2108	HIGH	Critical	The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the negative zero issue.	openssl	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-553
5588	CVE-2016-2107	LOW	Medium	The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session, NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.	openssl	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-552
5589	CVE-2016-2106	MEDIUM	High	Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.	openssl	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-556

	A	B	C	D	E	F	G	H	I	J	K	L	M
5590	CVE-2016-2105	MEDIUM	High	Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.	openssl	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-555
5591	CVE-2016-2099	HIGH	Critical	Use-after-free vulnerability in validators/DTD/DTDScanner.cpp in Apache Xerces C++ 3.1.3 and earlier does not properly handle exceptions raised in the XMLReader class, which allows context-dependent attackers to have unspecified impact via an invalid character in an XML document.	xerces-c	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-567
5592	CVE-2016-2090	HIGH	Critical	libbsd 0.8.1 and earlier contains a buffer overflow in the function fgetwln(). An if checks if it is necessary to reallocate memory in the target buffer. However this check is off by one, therefore an out of bounds write happens. (backtick) characters in a print job.	libbsd	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-308
5593	CVE-2016-2089	MEDIUM	Medium	The jas_matrix_clip function in jas_seq.c in JasPer 1.900.1 allows remote attackers to cause a denial of service (invalid read and application crash) via a crafted JPEG 2000 image.	jasper	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-264
5594	CVE-2016-2088	MEDIUM	Medium	resolver.c in named in ISC BIND 9.10.x before 9.10.3-P4, when DNS cookies are enabled, allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed packet with more than one cookie option.	bind	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-367
5595	CVE-2016-2085	LOW	Medium	The evm_verify_hmac function in security/integrity/evm/evm_main.c in the Linux kernel before 4.5 does not properly copy data, which makes it easier for local users to forge MAC values via a timing side-channel attack.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-576
5596	CVE-2016-2074	HIGH	Critical	Buffer overflow in lib/flow.c in ovs-vswitchd in Open vSwitch 2.2.x and 2.3.x before 2.3.3 and 2.4.x before 2.4.1 allows remote attackers to execute arbitrary code via crafted MPLS packets, as demonstrated by a long string in an ovs-appctl command.	openvswitch	Unchanged	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4414
5597	CVE-2016-2073	MEDIUM	Medium	The htmlParseNameComplex function in HTMLparser.c in libxml2 allows attackers to cause a denial of service (out-of-bounds read) via a crafted XML document.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-230
5598	CVE-2016-2070	HIGH	High	The tcp_cwnd_reduction function in net/ipv4/tcp_input.c in the Linux kernel before 4.3.5 allows remote attackers to cause a denial of service (divide-by-zero error and system crash) via crafted TCP traffic.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-630
5599	CVE-2016-2069	MEDIUM	High	Race condition in arch/x86/mm/tlb.c in the Linux kernel before 4.4.1 allows local users to gain privileges by triggering access to a paging structure by a different CPU.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-674
5600	CVE-2016-2065	HIGH	Critical	sound/soc/msm/qdsp6v2/msm-audio-effects-q6-v2.c in the MSM QDSP6 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (out-of-bounds write and memory corruption) or possibly have unspecified other impact via a crafted application that makes an ioctl call triggering incorrect use of a parameters pointer.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1387
5601	CVE-2016-2064	HIGH	High	sound/soc/msm/qdsp6v2/msm-audio-effects-q6-v2.c in the MSM QDSP6 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted application that makes an ioctl call specifying many commands.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1426
5602	CVE-2016-2063	HIGH	Critical	Stack-based buffer overflow in the supply_lm_input_write function in drivers/thermal/supply_lm_core.c in the MSM Thermal driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted application that sends a large amount of data through the debugfs interface.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1396
5603	CVE-2016-2053	HIGH	Medium	The asn1_ber_decoder function in lib/asn1_decoder.c in the Linux kernel before 4.3 allows attackers to cause a denial of service (panic) via an ASN.1 BER file that lacks a public key, leading to mishandling by the public_key_verify_signature function in crypto/asymmetric_keys/public_key.c.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-639
5604	CVE-2016-2052	MEDIUM	High	Multiple unspecified vulnerabilities in HarfBuzz before 1.0.6, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	harfbuzz	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-205
5605	CVE-2016-2047	MEDIUM	Medium	The ssl_verify_server_cert function in sql-common/client.c in MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10, Oracle MySQL, and Percona Server do not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a /CN= string in a field in a certificate, as demonstrated by /OU=/CN=bar.com/CN=foo.com.	mariadb	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-231
5606	CVE-2016-2045	LOW	Medium	Cross-site scripting (XSS) vulnerability in the SQL editor in phpMyAdmin 4.5.x before 4.5.4 allows remote authenticated users to inject arbitrary web script or HTML via a SQL query that triggers JSON data in a response.	phpMyAdmin	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-293
5607	CVE-2016-2044	MEDIUM	Medium	libraries/sql-parser/autoload.php in the SQL parser in phpMyAdmin 4.5.x before 4.5.4 allows remote attackers to obtain sensitive information via a crafted request, which reveals the full path in an error message.	phpMyAdmin	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-317
5608	CVE-2016-2043	LOW	Medium	Cross-site scripting (XSS) vulnerability in the goToFinish1NF function in js/normalization.js in phpMyAdmin 4.4.x before 4.4.15.3 and 4.5.x before 4.5.4 allows remote authenticated users to inject arbitrary web script or HTML via a table name to the normalization page.	phpMyAdmin	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-314

	A	B	C	D	E	F	G	H	I	J	K	L	M
5609	CVE-2016-2042	MEDIUM	Medium	phpMyAdmin 4.4.x before 4.4.15.3 and 4.5.x before 4.5.4 allows remote attackers to obtain sensitive information via a crafted request to (1) libraries/phpseclib/Crypt/AES.php or (2) libraries/phpseclib/Crypt/Rijndael.php, which reveals the full path in an error message.	phpMyAdmin	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-312
5610	CVE-2016-2041	MEDIUM	High	libraries/common.inc.php in phpMyAdmin 4.0.x before 4.0.10.13, 4.4.x before 4.4.15.3, and 4.5.x before 4.5.4 does not use a constant-time algorithm for comparing CSRF tokens, which makes it easier for remote attackers to bypass intended access restrictions by measuring time differences.	phpMyAdmin	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-306
5611	CVE-2016-2040	LOW	Medium	Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.13, 4.4.x before 4.4.15.3, and 4.5.x before 4.5.4 allow remote authenticated users to inject arbitrary web script or HTML via a (1) table name, (2) SET value, (3) search query, or (4) hostname in a Location header.	phpMyAdmin	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-300
5612	CVE-2016-2039	MEDIUM	Medium	libraries/session.inc.php in phpMyAdmin 4.0.x before 4.0.10.13, 4.4.x before 4.4.15.3, and 4.5.x before 4.5.4 does not properly generate CSRF token values, which allows remote attackers to bypass intended access restrictions by predicting a value.	phpMyAdmin	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-295
5613	CVE-2016-2038	MEDIUM	Medium	phpMyAdmin 4.0.x before 4.0.10.13, 4.4.x before 4.4.15.3, and 4.5.x before 4.5.4 allows remote attackers to obtain sensitive information via a crafted request, which reveals the full path in an error message.	phpMyAdmin	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-297
5614	CVE-2016-2037	MEDIUM	Medium	The cpio_safer_name_suffix function in util.c in cpio 2.11 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted cpio file.	cpio	Unchanged	8.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-299
5615	CVE-2016-1981	LOW	Medium	QEMU (aka Quick Emulator) built with the e1000 NIC emulation support is vulnerable to an infinite loop issue. It could occur while processing data via transmit or receive descriptors, provided the initial receive/transmit descriptor head (TDH/RDH) is set outside the allocated descriptor buffer. A privileged user inside guest could use this flaw to crash the QEMU instance resulting in DoS.	qemu	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2966
5616	CVE-2016-1979	MEDIUM	High	Use-after-free vulnerability in the PK11_ImportDERPrivateKeyInfoAndReturnKey function in Mozilla Network Security Services (NSS) before 3.21.1, as used in Mozilla Firefox before 45.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted key data with DER encoding.CWE-416: Use After Free	nss	Unchanged	8.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-405
5617	CVE-2016-1978	HIGH	High	Use-after-free vulnerability in the ssl3_HandleECDHServerKeyExchange function in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Firefox before 44.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact by making an SSL (1) DHE or (2) ECDHE handshake at a time of high memory consumption.CWE-416: Use After Free	nss	Unchanged	8.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-398
5618	CVE-2016-1972	MEDIUM	High	Race condition in libvpx in Mozilla Firefox before 45.0 on Windows might allow remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.CWE-416: Use After Free	libvpx	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-394
5619	CVE-2016-1950	MEDIUM	High	Heap-based buffer overflow in Mozilla Network Security Services (NSS) before 3.19.2.3 and 3.20.x and 3.21.x before 3.21.1, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to execute arbitrary code via crafted ASN.1 data in an X.509 certificate.	nss	Unchanged	8.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-408
5620	CVE-2016-1927	MEDIUM	High	The suggestPassword function in js/functions.js in phpMyAdmin 4.0.x before 4.0.10.13, 4.4.x before 4.4.15.3, and 4.5.x before 4.5.4 relies on the Math.random JavaScript function, which makes it easier for remote attackers to guess passwords via a brute-force approach.	phpMyAdmin	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-311
5621	CVE-2016-1924	MEDIUM	Medium	The opj_tgt_reset function in OpenJpeg 2016.1.18 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG 2000 image.	openjpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-261
5622	CVE-2016-1923	MEDIUM	Medium	Heap-based buffer overflow in the opj_j2k_update_image_data function in OpenJpeg 2016.1.18 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG 2000 image.	openjpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-254
5623	CVE-2016-1922	LOW	Medium	QEMU (aka Quick Emulator) built with the TPR optimization for 32-bit Windows guests support is vulnerable to a null pointer dereference flaw. It occurs while doing I/O port write operations via hmp interface. In that, 'current_cpu' remains null, which leads to the null pointer dereference. A user or process could use this flaw to crash the QEMU instance, resulting in DoS issue.	qemu	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2992
5624	CVE-2016-1908	HIGH	Critical	It was discovered that OpenSSH client did not correctly handle situations when untrusted X11 forwarding was requested and generation of the untrusted authentication cookie failed. The ssh client continued by generating fake authentication cookie and allowed remote X clients to connect the local X server. The decision if client connection was accepted was delegated to the X server which, depending on its configuration, could allow clients to open trusted X connection. This would lead to remote X clients having more privileged access to the local X server than intended.	openssh	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3837

	A	B	C	D	E	F	G	H	I	J	K	L	M
5625	CVE-2016-1907	MEDIUM	Medium	The ssh_packet_read_poll2 function in packet.c in OpenSSH before 7.1p2 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted network traffic.	openssh	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-174
5626	CVE-2016-1904	HIGH	High	Multiple integer overflows in ext/standard/exec.c in PHP 7.x before 7.0.2 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a long string to the (1) php_escape_shell_cmd or (2) php_escape_shell_arg function, leading to a heap-based buffer overflow.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-208
5627	CVE-2016-1903	MEDIUM	Critical	The gdImageRotateInterpolated function in ext/gd/libgd/gd_interpolation.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a large bgd_color argument to the imagerotate function.	php	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-175
5628	CVE-2016-1898	MEDIUM	Medium	FFmpeg 2.x allows remote attackers to conduct cross-origin attacks and read arbitrary files by using the subfile protocol in an HTTP Live Streaming (HLS) M3U8 file, leading to an external HTTP request in which the URL string contains an arbitrary line of a local file.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-169
5629	CVE-2016-1897	MEDIUM	Medium	FFmpeg 2.x allows remote attackers to conduct cross-origin attacks and read arbitrary files by using the concat protocol in an HTTP Live Streaming (HLS) M3U8 file, leading to an external HTTP request in which the URL string contains the first line of a local file.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-199
5630	CVE-2016-1867	MEDIUM	Medium	The jpc_pi_nextcprl function in JasPer 1.900.1 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG 2000 image.	jasper	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-173
5631	CVE-2016-1864	MEDIUM	Medium	The XSS auditor in WebKit, as used in Apple iOS before 9.3 and Safari before 9.1, does not properly handle redirects in block mode, which allows remote attackers to obtain sensitive information via a crafted URL.	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-922
5632	CVE-2016-1859	MEDIUM	High	The WebKit Canvas implementation in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-747
5633	CVE-2016-1858	MEDIUM	Medium	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, improperly tracks taint attributes, which allows remote attackers to obtain sensitive information via a crafted web site.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-758
5634	CVE-2016-1857	MEDIUM	High	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1855, and CVE-2016-1856.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-774
5635	CVE-2016-1856	MEDIUM	High	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1855, and CVE-2016-1857.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-783
5636	CVE-2016-1855	MEDIUM	High	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1856, and CVE-2016-1857.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-706
5637	CVE-2016-1854	MEDIUM	High	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1855, CVE-2016-1856, and CVE-2016-1857.	webkit	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-717
5638	CVE-2016-1841	MEDIUM	High	libxslt, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	libxslt	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-786
5639	CVE-2016-1840	MEDIUM	High	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, and CVE-2016-1839.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-700
5640	CVE-2016-1839	MEDIUM	High	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, and CVE-2016-1840.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-692
5641	CVE-2016-1838	MEDIUM	High	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1839, and CVE-2016-1840.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-699
5642	CVE-2016-1837	MEDIUM	High	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1836, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-698

	A	B	C	D	E	F	G	H	I	J	K	L	M
5643	CVE-2016-1836	MEDIUM	High	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1834, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-697
5644	CVE-2016-1835	MEDIUM	High	libxml2, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-696
5645	CVE-2016-1834	MEDIUM	High	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1833, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-695
5646	CVE-2016-1833	MEDIUM	High	libxml2, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2016-1834, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, and CVE-2016-1840.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-694
5647	CVE-2016-1786	MEDIUM	Medium	The Page Loading implementation in WebKit in Apple iOS before 9.3 and Safari before 9.1 mishandles HTTP responses with a 3xx (aka redirection) status code, which allows remote attackers to spoof the displayed URL, bypass the Same Origin Policy, and obtain sensitive cached information via a crafted web site.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-409
5648	CVE-2016-1785	MEDIUM	Medium	The Page Loading implementation in WebKit in Apple iOS before 9.3 and Safari before 9.1 mishandles character encoding during access to cached data, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-402
5649	CVE-2016-1784	MEDIUM	Medium	The History implementation in WebKit in Apple iOS before 9.3, Safari before 9.1, and tvOS before 9.2 allows remote attackers to cause a denial of service (resource consumption and application crash) via a crafted web site.	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-390
5650	CVE-2016-1783	HIGH	High	WebKit in Apple iOS before 9.3, Safari before 9.1, and tvOS before 9.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-404
5651	CVE-2016-1782	MEDIUM	Medium	WebKit in Apple iOS before 9.3 and Safari before 9.1 does not properly restrict redirects that specify a TCP port number, which allows remote attackers to bypass intended port restrictions via a crafted web site.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-397
5652	CVE-2016-1781	MEDIUM	Medium	WebKit in Apple iOS before 9.3 and Safari before 9.1 mishandles attachment URLs, which makes it easier for remote web servers to track users via unspecified vectors.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-400
5653	CVE-2016-1780	MEDIUM	Medium	WebKit in Apple iOS before 9.3 does not prevent hidden web views from reading orientation and motion data, which allows remote attackers to obtain sensitive information about a device's physical environment via a crafted web site.	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-395
5654	CVE-2016-1779	MEDIUM	Medium	WebKit in Apple iOS before 9.3 and Safari before 9.1 allows remote attackers to bypass the Same Origin Policy and obtain physical-location data via a crafted geolocation request.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-388
5655	CVE-2016-1778	HIGH	High	WebKit in Apple iOS before 9.3 and Safari before 9.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-410
5656	CVE-2016-1762	HIGH	Critical	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.	libxml2	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1457
5657	CVE-2016-1728	MEDIUM	Medium	The Cascading Style Sheets (CSS) implementation in Apple iOS before 9.2.1 and Safari before 9.0.3 mishandles the a:visited button selector during height processing, which makes it easier for remote attackers to obtain sensitive browser-history information via a crafted web site.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-414
5658	CVE-2016-1727	HIGH	High	WebKit, as used in Apple iOS before 9.2.1, Safari before 9.0.3, and tvOS before 9.1.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1724.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-259
5659	CVE-2016-1726	HIGH	High	WebKit, as used in Apple iOS before 9.2.1 and Safari before 9.0.3, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1723 and CVE-2016-1725.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-228
5660	CVE-2016-1725	HIGH	High	WebKit, as used in Apple iOS before 9.2.1 and Safari before 9.0.3, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1723 and CVE-2016-1726.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-248
5661	CVE-2016-1724	HIGH	High	WebKit, as used in Apple iOS before 9.2.1, Safari before 9.0.3, and tvOS before 9.1.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1727.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-223
5662	CVE-2016-1723	HIGH	High	WebKit, as used in Apple iOS before 9.2.1 and Safari before 9.0.3, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1725 and CVE-2016-1726.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-243

	A	B	C	D	E	F	G	H	I	J	K	L	M
5663	CVE-2016-1714	MEDIUM	High	The (1) fw_cfg_write and (2) fw_cfg_read functions in hw/nvram/fw_cfg.c in QEMU before 2.4, when built with the Firmware Configuration device emulation support, allow guest OS users with the CAP_SYS_RAWIO privilege to cause a denial of service (out-of-bounds read or write access and process crash) or potentially execute arbitrary code via an invalid current entry value in a firmware configuration.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-430
5664	CVE-2016-1684	MEDIUM	High	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles the i format token for xsl:number data, which allows remote attackers to cause a denial of service (integer overflow or resource consumption) or possibly have unspecified other impact via a crafted document.CWE-190: Integer Overflow or Wraparound	libxslt	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-843
5665	CVE-2016-1683	MEDIUM	High	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles namespace nodes, which allows remote attackers to cause a denial of service (out-of-bounds heap memory access) or possibly have unspecified other impact via a crafted document.	libxslt	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-845
5666	CVE-2016-1681	MEDIUM	High	Heap-based buffer overflow in the opj_j2k_read_SPCod_SPCoc function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 51.0.2704.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.	openjpeg	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-831
5667	CVE-2016-1663	MEDIUM	High	The SerializedScriptValue::transferArrayBuffers function in WebKit/Source/bindings/core/v8/SerializedScriptValue.cpp in the V8 bindings in Blink, as used in Google Chrome before 50.0.2661.94, mishandles certain array-buffer data structures, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site.	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-602
5668	CVE-2016-1645	HIGH	High	Multiple integer signedness errors in the opj_j2k_update_image_data function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 49.0.2623.87, allow remote attackers to cause a denial of service (incorrect cast and out-of-bounds write) or possibly have unspecified other impact via crafted JPEG 2000 data.	openjpeg	Unchanged	8.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-391
5669	CVE-2016-1644	HIGH	High	WebKit/Source/core/layout/LayoutObject.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly restrict relayout scheduling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted HTML document.CWE-416: Use After Free	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-396
5670	CVE-2016-1643	HIGH	High	The ImageInputType::ensurePrimaryContent function in WebKit/Source/core/html/forms/ImageInputType.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly maintain the user agent shadow DOM, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage type confusion.	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-393
5671	CVE-2016-1634	HIGH	High	Use-after-free vulnerability in the StyleResolver::appendCSSStyleSheet function in WebKit/Source/core/css/resolver/StyleResolver.cpp in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that triggers Cascading Style Sheets (CSS) style invalidation during a certain subtree-removal action.CWE-416: Use After Free	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-371
5672	CVE-2016-1630	MEDIUM	High	The ContainerNode::parserRemoveChild function in WebKit/Source/core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 49.0.2623.75, mishandles widget updates, which makes it easier for remote attackers to bypass the Same Origin Policy via a crafted web site.	webkit	Unchanged	Vulnerable	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-353
5673	CVE-2016-1628	MEDIUM	Medium	pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, does not validate a certain precision value, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via a crafted JPEG 2000 image in a PDF document, related to the opj_pi_next_rpcl, opj_pi_next_pcrl, and opj_pi_next_cprl functions.	openjpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-315
5674	CVE-2016-1626	MEDIUM	Medium	The opj_pi_update_decode_poc function in pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, miscalculates a certain layer index value, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.	openjpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-309
5675	CVE-2016-1585	High	CRITICAL	In all versions of AppArmor mount rules are accidentally widened when compiled.	apparmor	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4015
5676	CVE-2016-1583	HIGH	High	The ecryptfs_privileged_open function in fs/ecryptfs/kthread.c in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (stack memory consumption) via vectors involving crafted mmap calls for /proc pathnames, leading to recursive pagefault handling.	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-927
5677	CVE-2016-1577	MEDIUM	High	Double free vulnerability in the jas_iccattrval_destroy function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted ICC color profile in a JPEG 2000 image file, a different vulnerability than CVE-2014-8137.	jasper	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-449

	A	B	C	D	E	F	G	H	I	J	K	L	M
5678	CVE-2016-1576	HIGH	High	The overlayfs implementation in the Linux kernel through 4.5.2 does not properly restrict the mount namespace, which allows local users to gain privileges by mounting an overlayfs filesystem on top of a FUSE filesystem, and then executing a crafted setuid program.	linux	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-574
5679	CVE-2016-1575	HIGH	High	The overlayfs implementation in the Linux kernel through 4.5.2 does not properly maintain POSIX ACL xattr data, which allows local users to gain privileges by leveraging a group-writable setgid directory.	linux	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-617
5680	CVE-2016-1572	MEDIUM	High	mount.ecryptfs_private.c in eCryptfs-utils does not validate mount destination filesystem types, which allows local users to gain privileges by mounting over a nonstandard filesystem, as demonstrated by /proc/$pid.	ecryptfs-utils	Unchanged	8.0.0.3	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-166
5681	CVE-2016-1568	HIGH	High	A use-after-free flaw was found in the way QEMU's IDE AHCI emulator processed certain AHCI Native Command Queuing (NCQ) AIO commands. A privileged guest user could use this flaw to crash the QEMU process instance or, potentially, execute arbitrary code on the host with privileges of the QEMU process.	qemu	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-282
5682	CVE-2016-1551	LOW	Low	While the majority OSes implement martian packet filtering in their network stack, at least regarding 127.0.0.0/8, a rare few will allow packets claiming to be from 127.0.0.0/8 that arrive over physical network. On these OSes, if ntpd is configured to use a reference clock an attacker can inject packets over the network that look like they are coming from that reference clock.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-834
5683	CVE-2016-1550	MEDIUM	Medium	An exploitable vulnerability exists in the message authentication functionality of Network Time Protocol libntp. An attacker can send a series of crafted messages to attempt to recover the message digest key.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-824
5684	CVE-2016-1549	MEDIUM	Medium	ntpd can be vulnerable to Sybil attacks. If a system is set up to use a trustedkey and if one is not using the feature introduced in ntp-4.2.8p6 allowing an optional 4th field in the ntp.keys file to specify which IPs can serve time, a malicious authenticated peer -- i.e. one where the attacker knows the private symmetric key -- can create arbitrarily-many ephemeral associations in order to win the clock selection of ntpd and modify a victim's clock.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-813
5685	CVE-2016-1548	MEDIUM	High	ntpd supports an interleaved mode to allow the protocol to exchange transmit timestamps that were captured after the packet was sent in symmetric associations and broadcast modes. It can be enabled in the configuration file, but it's also enabled automatically when a packet received from the source is detected to be in the interleaved mode. The detection compares the origin timestamp in the packet to the previous local receive timestamp. The interleaved mode is enabled even in client associations, even though it makes no sense there.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-832
5686	CVE-2016-1547	MEDIUM	Medium	An off-path attacker can cause a preemptable client association to be demobilized by sending a crypto NAK packet to a victim client with a spoofed source address of an existing associated peer. This is true even if authentication is enabled. Furthermore, if the attacker keeps sending crypto NAK packets, for example every one second, the victim never has a chance to reestablish the association and synchronize time with the legitimate server.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-840
5687	CVE-2016-1546	MEDIUM	Medium	The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1106
5688	CVE-2016-1541	MEDIUM	High	Heap-based buffer overflow in the zip_read_mac_metadata function in archive_read_support_format_zip.c in libarchive before 3.2.0 allows remote attackers to execute arbitrary code via crafted entry-size values in a ZIP archive.	libarchive	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-575
5689	CVE-2016-1517	MEDIUM	Medium	OpenCV 3.0.0 allows remote attackers to cause a denial of service (segfault) via vectors involving corrupt chunks.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-3921
5690	CVE-2016-1516	MEDIUM	High	OpenCV 3.0.0 has a double free issue that allows attackers to execute arbitrary code.	opencv	Unchanged	Won't Fix	9.0.0.11	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-3970
5691	CVE-2016-1515			A use-after-free / double-free vulnerability can occur in libebml master branch while parsing Track elements of the MKV container.	libebml	Updated	8.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2995
5692	CVE-2016-1514			A specially crafted unicode string in libebml master branch can cause an off-by-few read on the heap in unicode string parsing code in libebml. This issue can potentially be used for information leaks.	libebml	Updated	8.0.0.14	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-2990
5693	CVE-2016-1504	MEDIUM	High	dhcpcd before 6.10.0 allows remote attackers to cause a denial of service (invalid read and crash) via vectors related to the option length.	dhcpcd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3249
5694	CVE-2016-1494	MEDIUM	Medium	The verify function in the RSA package for Python (Python-RSA) before 3.3 allows attackers to spoof signatures with a small public exponent via crafted signature padding, aka a BERserk attack.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-160
5695	CVE-2016-1372	MEDIUM	Medium	ClamAV (aka Clam AntiVirus) before 0.99.2 allows remote attackers to cause a denial of service (application crash) via a crafted 7z file.	clamav	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1725
5696	CVE-2016-1371	MEDIUM	Medium	ClamAV (aka Clam AntiVirus) before 0.99.2 allows remote attackers to cause a denial of service (application crash) via a crafted mew packer executable.	clamav	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1726
5697	CVE-2016-1286	MEDIUM	High	named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted signature record for a DNAME record, related to db.c and resolver.c.	bind	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-352

	A	B	C	D	E	F	G	H	I	J	K	L	M
5698	CVE-2016-1285	MEDIUM	Medium	named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed packet to the rndc (aka control channel) interface, related to alist.c and sexpr.c.	bind	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-370
5699	CVE-2016-1284	LOW	Medium	rdataset.c in ISC BIND 9 Supported Preview Edition 9.9.8-S before 9.9.8-S5, when nxdomain-redirect is enabled, allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via crafted flag values in a query.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-237
5700	CVE-2016-1283	HIGH	Critical	The pcre_compile2 function in pcre_compile.c in PCRE 8.38 mishandles the /((?:F?+(?:^(?(R)a+\)\{99}-))(?J)(?'R'(?'R'<((?'RR'(?'R'\)|9?)?2))\?.)(?'R'(?'R'\)\{99|(.(?|(?'R')(\k'R')|((?'R'))|H'R'R)(H'R)))))/ pattern and related patterns with named subgroups, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-103
5701	CVE-2016-1252	MEDIUM	Medium	The apt package in Debian jessie before 1.0.9.8.4, in Debian unstable before 1.4~beta2, in Ubuntu 14.04 LTS before 1.0.1ubuntu2.17, in Ubuntu 16.04 LTS before 1.2.15ubuntu0.2, and in Ubuntu 16.10 before 1.3.2ubuntu0.1 allows man-in-the-middle attackers to bypass a repository-signing protection mechanism by leveraging improper error handling when validating InRelease file signatures.	apt	Unchanged	8.0.0.25	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2768
5702	CVE-2016-1248	MEDIUM	High	vim before patch 8.0.0056 does not properly validate values for the 'filetype', 'syntax' and 'keymap' options, which may result in the execution of arbitrary code if a file with a specially crafted modeline is opened.	vim	Unchanged	8.0.0.12	9.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2397
5703	CVE-2016-1247	HIGH	High	The nginx package before 1.6.2-5+deb8u3 on Debian jessie and the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10 allow local users with access to the web server user account to gain root privileges via a symlink attack on the error log.	nginx	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2779
5704	CVE-2016-1245	HIGH	Critical	It was discovered that the zebra daemon in Quagga before 1.0.20161017 suffered from a stack-based buffer overflow when processing IPv6 Neighbor Discovery messages. The root cause was relying on BUFSIZ to be compatible with a message size; however, BUFSIZ is system-dependent.	quagga	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3412
5705	CVE-2016-1238	HIGH	High	(1) cpan/Archive-Tar/bin/ptar, (2) cpan/Archive-Tar/bin/ptardiff, (3) cpan/Archive-Tar/bin/ptargrep, (4) cpan/CPAN/scripts/cpan, (5) cpan/Digest-SHA/shasum, (6) cpan/Encode/bin/enc2xs, (7) cpan/Encode/bin/encguess, (8) cpan/Encode/bin/piconv, (9) cpan/Encode/bin/ucmlint, (10) cpan/Encode/bin/unidump, (11) cpan/ExtUtils-MakeMaker/bin/instmodsh, (12) cpan/IO-Compress/bin/zipdetails, (13) cpan/JSON-PP/bin/json_pp, (14) cpan/Test-Harness/bin/prove, (15) dist/ExtUtils-ParseXS/lib/ExtUtils/xsubpp, (16) dist/Module-CoreList/corelist, (17) ext/Pod-Html/bin/pod2html, (18) utils/c2ph.PL, (19) utils/h2ph.PL, (20) utils/h2xs.PL, (21) utils/libnetcfg.PL, (22) utils/perlbug.PL, (23) utils/perldoc.PL, (24) utils/perlivp.PL, and (25) utils/splain.PL in Perl 5.x before 5.22.3-RC2 and 5.24 before 5.24.1-RC2 do not properly remove . (period) characters from the end of the includes directory array, which might allow local users to gain privileges via a Trojan horse module under the current working directory.	perl	Unchanged	8.0.0.10	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1373
5706	CVE-2016-1237	MEDIUM	Medium	nfsd in the Linux kernel through 4.6.3 allows local users to bypass intended file-permission restrictions by setting a POSIX ACL, related to nfs2acl.c, nfs3acl.c, and nfs4acl.c.	linux	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-942
5707	CVE-2016-1234	MEDIUM	High	Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name.	glibc	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-827
5708	CVE-2016-10907	Medium	HIGH	An issue was discovered in drivers/iio/dac/ad5755.c in the Linux kernel before 4.8.6. There is an out of bounds write in the function ad5755_parse_dt.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4708
5709	CVE-2016-10906	Medium	HIGH	An issue was discovered in drivers/net/ethernet/arc/emac_main.c in the Linux kernel before 4.5. A use-after-free is caused by a race condition between the functions arc_emac_tx and arc_emac_tx_clean.	linux	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4707
5710	CVE-2016-10905	Medium	HIGH	An issue was discovered in fs/gfs2/rgrp.c in the Linux kernel before 4.8. A use-after-free is caused by the functions gfs2_clear_rgrpd and read_rindex_entry.	linux	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4712
5711	CVE-2016-10764	HIGH	CRITICAL	In the Linux kernel before 4.9.6, there is an off by one in the drivers/mtd/spi-nor/cadence-quadspi.c cqspi_setup_flash() function. There are CQSPI_MAX_CHIPSELECT elements in the ->f_pdata array so the > should be >= instead.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4546
5712	CVE-2016-10746	Medium	HIGH	libvirt-domain.c in libvirt before 1.3.1 supports virDomainGetTime API calls by guest agents with an RO connection, even though an RW connection was supposed to be required, a different vulnerability than CVE-2019-3886.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3962
5713	CVE-2016-10743	Medium	HIGH	hostapd before 2.6 does not prevent use of the low-quality PRNG that is reached by an os_random() function call.	hostapd	Unchanged	8.0.0.30	9.0.0.21	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	LIN1018-3755
5714	CVE-2016-10742	Medium	MEDIUM	Zabbix before 2.2.21rc1, 3.x before 3.0.13rc1, 3.1.x and 3.2.x before 3.2.10rc1, and 3.3.x and 3.4.x before 3.4.4rc1 allows open redirect via the request parameter.	zabbix	Unchanged	Vulnerable	Vulnerable	Not vulnerable	Vulnerable	10.19.45.1	Not vulnerable	LIN1018-3753

	A	B	C	D	E	F	G	H	I	J	K	L	M
5715	CVE-2016-10741	Medium	MEDIUM	In the Linux kernel before 4.9.3, fs/xfs/xfs_aops.c allows local users to cause a denial of service (system crash) because there is a race condition between direct and memory-mapped I/O (associated with a hole) that is handled with BUG_ON instead of an I/O failure.	linux	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3547
5716	CVE-2016-10739	Medium	MEDIUM	In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a string that contained an IPv4 address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume that it had parsed a valid string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.	glibc	Unchanged	8.0.0.30	9.0.0.21	10.17.41.15	10.18.44.6	Not vulnerable	Not vulnerable	LIN1018-3494
5717	CVE-2016-10728	MEDIUM	MEDIUM	An issue was discovered in Suricata before 3.1.2. If an ICMPv4 error packet is received as the first packet on a flow in the to_client direction, it confuses the rule grouping lookup logic. The toclient inspection will then continue with the wrong rule group. This can lead to missed detection.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4420
5718	CVE-2016-10727	MEDIUM	CRITICAL	camel/providers/imapx/camel-imapx-server.c in the IMAPx component in GNOME evolution-data-server before 3.21.2 proceeds with cleartext data containing a password if the client wishes to use STARTTLS but the server will not use STARTTLS, which makes it easier for remote attackers to obtain sensitive information by sniffing the network. The server code was intended to report an error and not proceed, but the code was written incorrectly.	evolution-data-server	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4386
5719	CVE-2016-10723	MEDIUM	MEDIUM	** DISPUTED ** An issue was discovered in the Linux kernel through 4.17.2. Since the page allocator does not yield CPU resources to the owner of the oom_lock mutex, a local unprivileged user can trivially lock up the system forever by wasting CPU resources from the page allocator (e.g., via concurrent page fault events) when the global OOM killer is invoked. NOTE: the software maintainer has not accepted certain proposed patches, in part because of a viewpoint that the underlying problem is non-trivial to handle.	linux	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3679
5720	CVE-2016-10714	HIGH	CRITICAL	In zsh before 5.3, an off-by-one error resulted in undersized buffers that were intended to support PATH_MAX characters.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3579
5721	CVE-2016-10713	MEDIUM	Medium	An issue was discovered in GNU patch before 2.7.6. Out-of-bounds access within pch_write_line() in pch.c can possibly lead to DoS via a crafted input file.	patch	Unchanged	8.0.0.26	9.0.0.15	10.17.41.5	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3434
5722	CVE-2016-10712	MEDIUM	High	In PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3, all of the return values of stream_get_meta_data can be controlled if the input can be controlled (e.g., during file uploads). For example, a $uri = stream_get_meta_data(fopen($file, r)) ['uri'] call mishandles the case where $file is data:text/plain;uri=eviluri, -- in other words, metadata can be set by an attacker.	php	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3438
5723	CVE-2016-10708	MEDIUM	High	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.	openssh	Unchanged	8.0.0.25	9.0.0.15	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3189
5724	CVE-2016-10517	MEDIUM	High	networking.c in Redis before 3.2.7 allows Cross Protocol Scripting because it lacks a check for POST and Host: strings, which are not valid in the Redis protocol (but commonly occur when an attack triggers an HTTP request to the Redis TCP port).	redis	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5718
5725	CVE-2016-10507	Medium	Medium	Integer overflow vulnerability in the bmp24toimage function in convertbmp.c in OpenJPEG before 2.2.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted bmp file.	openjpeg	Unchanged	Won't Fix	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5388
5726	CVE-2016-10506	Medium	Medium	Division-by-zero vulnerabilities in the functions opj_pi_next_cprl, opj_pi_next_pcrl, and opj_pi_next_rpcl in pi.c in OpenJPEG before 2.2.0 allow remote attackers to cause a denial of service (application crash) via crafted j2k files.	openjpeg	Unchanged	Won't Fix	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5355
5727	CVE-2016-10504	Medium	Medium	Heap-based buffer overflow vulnerability in the opj_mqc_byteout function in mqc.c in OpenJPEG before 2.2.0 allows remote attackers to cause a denial of service (application crash) via a crafted bmp file.	openjpeg	Unchanged	Won't Fix	9.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5232
5728	CVE-2016-10397	MEDIUM	High	In PHP before 5.6.28 and 7.x before 7.0.13, incorrect handling of various URI components in the URL parser could be used by attackers to bypass hostname-specific URL checks, as demonstrated by evil.example.com:80#@good.example.com/ and evil.example.com:80?@good.example.com/ inputs to the parse_url function (implemented in the php_url_parse_ex function in ext/standard/url.c).	php	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4671
5729	CVE-2016-10396	HIGH	High	The racoon daemon in IPsec-Tools 0.8.2 contains a remotely exploitable computational-complexity attack when parsing and storing ISAKMP fragments. The implementation permits a remote attacker to exhaust computational resources on the remote endpoint by repeatedly sending ISAKMP fragment packets in a particular order such that the worst-case computational complexity is realized in the algorithm utilized to determine if reassembly of the fragments can take place.	ipsec-tools	Unchanged	8.0.0.20	9.0.0.9	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-4649
5730	CVE-2016-10377	MEDIUM	High	In Open vSwitch (OvS) 2.5.0, a malformed IP packet can cause the switch to read past the end of the packet buffer due to an unsigned integer underflow in `lib/flow.c` in the function `miniflow_extract`, permitting remote bypass of the access control list enforced by the switch.	openvswitch	Unchanged	8.0.0.20	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4437

	A	B	C	D	E	F	G	H	I	J	K	L	M
5731	CVE-2016-10371	MEDIUM	Medium	The TIFFWriteDirectoryTagCheckedRational function in tif_dirwrite.c in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted TIFF file.	libtiff	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4234
5732	CVE-2016-10350	MEDIUM	Medium	The archive_read_format_cab_read_header function in archive_read_support_format_cab.c in libarchive 3.2.2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file.	libarchive	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4195
5733	CVE-2016-10349	MEDIUM	Medium	The archive_le32dec function in archive_endian.h in libarchive 3.2.2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file.	libarchive	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4239
5734	CVE-2016-10328	HIGH	Critical	FreeType 2 before 2016-12-16 has an out-of-bounds write caused by a heap-based buffer overflow related to the cff_parser_run function in cff/cffparse.c.	freetype	Unchanged	8.0.0.18	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4032
5735	CVE-2016-10318	MEDIUM	Medium	A missing authorization check in the fscrypt_process_policy function in fs/crypto/policy.c in the ext4 and f2fs filesystem encryption support in the Linux kernel before 4.7.4 allows a user to assign an encryption policy to a directory owned by a different user, potentially creating a denial of service.	linux	Unchanged	8.0.0.19	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3903
5736	CVE-2016-10317	MEDIUM	High	The fill_threshhold_buffer function in base/gxht_thresh.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PostScript document.	ghostscript	Unchanged	8.0.0.25	9.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3951
5737	CVE-2016-10272	MEDIUM	High	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted TIFF image, related to WRITE of size 2048 and libtiff/tif_next.c:64:9.	tiff	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3813
5738	CVE-2016-10271	MEDIUM	High	tools/tiffcrop.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer over-read and buffer overflow) or possibly have unspecified other impact via a crafted TIFF image, related to READ of size 1 and libtiff/tif_fax3.c:413:13.	tiff	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3656
5739	CVE-2016-10270	MEDIUM	High	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted TIFF image, related to READ of size 8 and libtiff/tif_read.c:523:22.	tiff	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3704
5740	CVE-2016-10269	MEDIUM	High	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted TIFF image, related to READ of size 512 and libtiff/tif_unix.c:340:2.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3669
5741	CVE-2016-10268	MEDIUM	High	tools/tiffcp.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (integer underflow and heap-based buffer under-read) or possibly have unspecified other impact via a crafted TIFF image, related to READ of size 78490 and libtiff/tif_unix.c:115:23.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3646
5742	CVE-2016-10267	MEDIUM	Medium	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted TIFF image, related to libtiff/tif_ojpeg.c:816:8.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3724
5743	CVE-2016-10266	MEDIUM	Medium	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted TIFF image, related to libtiff/tif_read.c:351:22.	tiff	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3739
5744	CVE-2016-10255	MEDIUM	Medium	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted (1) sh_off or (2) sh_size ELF header value, which triggers a memory allocation failure.	elfutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3769
5745	CVE-2016-10254	MEDIUM	Medium	The allocate_elf function in common.h in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted ELF file, which triggers a memory allocation failure.	elfutils	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3641
5746	CVE-2016-10252	HIGH	High	Memory leak in the IsOptionMember function in MagickCore/option.c in ImageMagick before 6.9.2-2, as used in ODR-PadEnc and other products, allows attackers to trigger memory consumption.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3758
5747	CVE-2016-10251	MEDIUM	High	Integer overflow in the jpc_pi_nextcprl function in jpc_t2cod.c in JasPer before 1.900.20 allows remote attackers to have unspecified impact via a crafted file, which triggers use of an uninitialized value.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3818
5748	CVE-2016-10250	MEDIUM	High	The jp2_colr_destroy function in jp2_cod.c in JasPer before 1.900.13 allows remote attackers to cause a denial of service (NULL pointer dereference) by leveraging incorrect cleanup of JP2 box data on error. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8887.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3729
5749	CVE-2016-10249	MEDIUM	High	Integer overflow in the jpc_dec_tiledecode function in jpc_dec.c in JasPer before 1.900.12 allows remote attackers to have unspecified impact via a crafted image file, which triggers a heap-based buffer overflow.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3770
5750	CVE-2016-10248	MEDIUM	High	The jpc_tsfb_synthesize function in jpc_tsfb.c in JasPer before 1.900.9 allows remote attackers to cause a denial of service (NULL pointer dereference) via vectors involving an empty sequence.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3674
5751	CVE-2016-10244	MEDIUM	High	The parse_charstrings function in type1/t1load.c in FreeType 2 before 2.7 does not ensure that a font contains a glyph name, which allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted file.	freetype	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3531
5752	CVE-2016-10229	HIGH	Critical	udp.c in the Linux kernel before 4.5 allows remote attackers to execute arbitrary code via UDP traffic that triggers an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag.	linux	Unchanged	8.0.0.17	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3896

	A	B	C	D	E	F	G	H	I	J	K	L	M
5753	CVE-2016-10228	MEDIUM	Medium	The iconv program in the GNU C Library (aka glibc or libc6) 2.25 and earlier, when invoked with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.	glibc	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-3512
5754	CVE-2016-10220	MEDIUM	Medium	The gs_makewordimagedevice function in base/gsdevmem.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file that is mishandled in the PDF Transparency module.	ghostscript	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3910
5755	CVE-2016-10219	MEDIUM	Medium	The intersect function in base/gxfill.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted file.	ghostscript	Unchanged	8.0.0.18	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3917
5756	CVE-2016-10209	MEDIUM	Medium	The archive_wstring_append_from_mbs function in archive_string.c in libarchive 3.2.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted archive file.	libarchive	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3913
5757	CVE-2016-10208	MEDIUM	Medium	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.9.8 does not properly validate meta block groups, which allows physically proximate attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image.	linux	Unchanged	8.0.0.15	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3275
5758	CVE-2016-10207	MEDIUM	High	The Xvnc server in TigerVNC allows remote attackers to cause a denial of service (invalid memory access and crash) by terminating a TLS handshake early.	tigervnc	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3570
5759	CVE-2016-10200	MEDIUM	High	Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to gain privileges or cause a denial of service (use-after-free) by making multiple bind system calls without properly ascertaining whether a socket has the SOCK_ZAPPED status, related to net/l2tp/l2tp_ip.c and net/l2tp/l2tp_ip6.c.	linux	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3522
5760	CVE-2016-10199	MEDIUM	High	The qtdemux_tag_add_str_full function in gst/isomp4/qtdemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted tag value.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3426
5761	CVE-2016-10198	MEDIUM	Medium	The gst_aac_parse_sink_setcaps function in gst/audioparsers/gstaacparse.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted audio file.	gstreamer	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3407
5762	CVE-2016-10197	MEDIUM	High	The search_make_new function in evdns.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (out-of-bounds read) via an empty hostname.	libevent	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3760
5763	CVE-2016-10196	MEDIUM	High	Stack-based buffer overflow in the evutil_parse_sockaddr_port function in evutil.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (segmentation fault) via vectors involving a long string in brackets in the ip_as_string argument.	libevent	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3820
5764	CVE-2016-10195	HIGH	Critical	The name_parse function in evdns.c in libevent before 2.1.6-beta allows remote attackers to have unspecified impact via vectors involving the label_len variable, which triggers an out-of-bounds stack read.	libevent	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3636
5765	CVE-2016-10194	HIGH	Critical	The festivaltts4r gem for Ruby allows remote attackers to execute arbitrary commands via shell metacharacters in a string to the (1) to_speech or (2) to_mp3 method in lib/festivaltts4r/festival4r.rb.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3521
5766	CVE-2016-10193	HIGH	Critical	The espeak-ruby gem before 1.0.3 for Ruby allows remote attackers to execute arbitrary commands via shell metacharacters in a string to the speak, save, bytes or bytes_wav method in lib/espeak/speech.rb.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3515
5767	CVE-2016-10192	HIGH	Critical	Heap-based buffer overflow in ffserver.c in FFmpeg before 2.8.10, 3.0.x before 3.0.5, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 allows remote attackers to execute arbitrary code by leveraging failure to check chunk size.	ffmpeg	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3410
5768	CVE-2016-10191	HIGH	Critical	Heap-based buffer overflow in libavformat/rtmppkt.c in FFmpeg before 2.8.10, 3.0.x before 3.0.5, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 allows remote attackers to execute arbitrary code by leveraging failure to check for RTMP packet size mismatches.	ffmpeg	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3430
5769	CVE-2016-10190	HIGH	Critical	Heap-based buffer overflow in libavformat/http.c in FFmpeg before 2.8.10, 3.0.x before 3.0.5, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 allows remote web servers to execute arbitrary code via a negative chunk size in an HTTP response.	ffmpeg	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3413
5770	CVE-2016-10172	MEDIUM	Medium	The read_new_config_info function in open_utils.c in Wavpack before 5.1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WV file.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3684
5771	CVE-2016-10171	MEDIUM	Medium	The unreorder_channels function in cli/wvunpack.c in Wavpack before 5.1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WV file.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3714
5772	CVE-2016-10170	MEDIUM	Medium	The WriteCaffHeader function in cli/caff.c in Wavpack before 5.1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WV file.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3701
5773	CVE-2016-10169	MEDIUM	Medium	The read_code function in read_words.c in Wavpack before 5.1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WV file.	wavpack	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3667
5774	CVE-2016-10168	MEDIUM	High	Integer overflow in gd_io.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified impact via vectors involving the number of horizontal and vertical chunks in an image.	gd	Unchanged	8.0.0.17	9.0.0.6	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3699
5775	CVE-2016-10167	MEDIUM	Medium	The gdImageCreateFromGd2Ctx function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (application crash) via a crafted image file.	gd	Unchanged	8.0.0.17	9.0.0.6	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3748

	A	B	C	D	E	F	G	H	I	J	K	L	M
5776	CVE-2016-10166	HIGH	Critical	Integer underflow in the _gdContributionsAlloc function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified impact via vectors related to decrementing the u variable.	gd	Unchanged	8.0.0.17	9.0.0.6	10.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3716
5777	CVE-2016-10164	HIGH	Critical	Multiple integer overflows in libXpm before 3.5.12, when a program requests parsing XPM extensions on a 64-bit platform, allow remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via (1) the number of extensions or (2) their concatenated length in a crafted XPM file, which triggers a heap-based buffer overflow.	libxpm	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3207
5778	CVE-2016-10162	MEDIUM	High	The php_wddx_pop_element function in ext/wddx/wddx.c in PHP 7.0.x before 7.0.15 and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an inapplicable class name in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3266
5779	CVE-2016-10161	MEDIUM	High	The object_common1 function in ext/standard/var_unserializer.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via crafted serialized data that is mishandled in a finish_nested_data call.	php	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3228
5780	CVE-2016-10160	HIGH	Critical	Off-by-one error in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted PHAR archive with an alias mismatch.	php	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3170
5781	CVE-2016-10159	MEDIUM	High	Integer overflow in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory consumption or application crash) via a truncated manifest entry in a PHAR archive.	php	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3242
5782	CVE-2016-10158	MEDIUM	High	The exif_convert_any_to_int function in ext/exif/exif.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (application crash) via crafted EXIF data that triggers an attempt to divide the minimum representable negative integer by -1.	php	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3179
5783	CVE-2016-10156	HIGH	High	A flaw in systemd v228 in /src/basic/fs-util.c caused world writable suid files to be created when using the systemd timers features, allowing local attackers to escalate their privileges to root. This is fixed in v229.	systemd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3264
5784	CVE-2016-10155	MEDIUM	Medium	Memory leak in hw/watchdog/wdt_i6300esb.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.	qemu	Unchanged	8.0.0.16	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3808
5785	CVE-2016-10154	MEDIUM	Medium	The smbhash function in fs/cifs/smbencrypt.c in the Linux kernel 4.9.x before 4.9.1 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a scatterlist.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3245
5786	CVE-2016-10153	HIGH	High	The crypto scatterlist API in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging reliance on earlier net/ceph/crypto.c code.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3212
5787	CVE-2016-10150	HIGH	Critical	Use-after-free vulnerability in the kvm_ioctl_create_device function in virt/kvm/kvm_main.c in the Linux kernel before 4.8.13 allows host OS users to cause a denial of service (host OS crash) or possibly gain privileges via crafted ioctl calls on the /dev/kvm device.	linux	Unchanged	Not vulnerable	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3156
5788	CVE-2016-10147	MEDIUM	Medium	crypto/mcryptd.c in the Linux kernel before 4.8.15 allows local users to cause a denial of service (NULL pointer dereference and system crash) by using an AF_ALG socket with an incompatible algorithm, as demonstrated by mcryptd(md5).	linux	Unchanged	8.0.0.15	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3182
5789	CVE-2016-10146	HIGH	High	Multiple memory leaks in the caption and label handling code in ImageMagick allow remote attackers to cause a denial of service (memory consumption) via unspecified vectors.	imagemagick	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3763
5790	CVE-2016-10145	HIGH	Critical	Off-by-one error in coders/wpg.c in ImageMagick allows remote attackers to have unspecified impact via vectors related to a string copy.	imagemagick	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3737
5791	CVE-2016-10144	HIGH	Critical	coders/ipl.c in ImageMagick allows remote attackers to have unspecific impact by leveraging a missing malloc check.	imagemagick	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3766
5792	CVE-2016-10134	HIGH	Critical	SQL injection vulnerability in Zabbix before 2.2.14 and 3.0 before 3.0.4 allows remote attackers to execute arbitrary SQL commands via the toggle_ids array parameter in latest.php.	zabbix	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3414
5793	CVE-2016-10130	MEDIUM	Medium	The http_connect function in transports/http.c in libgit2 before 0.24.6 and 0.25.x before 0.25.1 might allow man-in-the-middle attackers to spoof servers by leveraging clobbering of the error variable.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3663
5794	CVE-2016-10129	MEDIUM	High	The Git Smart Protocol support in libgit2 before 0.24.6 and 0.25.x before 0.25.1 allows remote attackers to cause a denial of service (NULL pointer dereference) via an empty packet line.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3723
5795	CVE-2016-10128	HIGH	Critical	Buffer overflow in the git_pkt_parse_line function in transports/smart_pkt.c in the Git Smart Protocol support in libgit2 before 0.24.6 and 0.25.x before 0.25.1 allows remote attackers to have unspecified impact via a crafted non-flush packet.	libgit2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3645

	A	B	C	D	E	F	G	H	I	J	K	L	M
5796	CVE-2016-10124	MEDIUM	High	An issue was discovered in Linux Containers (LXC) before 2016-02-22. When executing a program via lxc-attach, the nonpriv session can escape to the parent session by using the TIOCSTI ioctl to push characters into the terminal's input buffer, allowing an attacker to escape the container.	lxc	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2975
5797	CVE-2016-10109	MEDIUM	High	Use-after-free vulnerability in pcsc-lite before 1.8.20 allows a remote attackers to cause denial of service (crash) via a command that uses cardsList after the handle has been released through the SCardReleaseContext function.	pcsc-lite	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3391
5798	CVE-2016-10095	MEDIUM	Medium	Stack-based buffer overflow in the _TIFFVGetField function in tif_dir.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (crash) via a crafted TIFF file.	libtiff	Unchanged	8.0.0.19	9.0.0.8	10.0.0.0	10.18.44.1	Not vulnerable	Not vulnerable	LIN9-3579
5799	CVE-2016-10094	MEDIUM	High	Off-by-one error in the t2p_readwrite_pdf_image_tile function in tools/tiff2pdf.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image.	libtiff	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3547
5800	CVE-2016-10093	MEDIUM	High	Integer overflow in tools/tiffcp.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image, which triggers a heap-based buffer overflow.	libtiff	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3526
5801	CVE-2016-10092	MEDIUM	High	Heap-based buffer overflow in the readContigStripsIntoBuffer function in tif_unix.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image.	libtiff	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3563
5802	CVE-2016-10088	MEDIUM	High	The sg implementation in the Linux kernel through 4.9 does not properly restrict write operations in situations where the KERNEL_DS option is set, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device, related to block/bsg.c and drivers/scsi/sg.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9576.	linux	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2977
5803	CVE-2016-10087	MEDIUM	High	The png_set_text_2 function in libpng 0.71 before 1.0.67, 1.2.x before 1.2.57, 1.4.x before 1.4.20, 1.5.x before 1.5.28, and 1.6.x before 1.6.27 allows context-dependent attackers to cause a NULL pointer dereference vectors involving loading a text chunk into a png structure, removing the text, and then adding another text chunk to the structure.	libpng	Unchanged	8.0.0.15	9.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3161
5804	CVE-2016-10071	MEDIUM	Medium	coders/mat.c in ImageMagick before 6.9.4-0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted mat file.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3517
5805	CVE-2016-10069	MEDIUM	Medium	coders/mat.c in ImageMagick before 6.9.4-5 allows remote attackers to cause a denial of service (application crash) via a mat file with an invalid number of frames.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3504
5806	CVE-2016-10068	MEDIUM	Medium	The MSL interpreter in ImageMagick before 6.9.6-4 allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted XML file.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3502
5807	CVE-2016-10067	MEDIUM	High	magick/memory.c in ImageMagick before 6.9.4-5 allows remote attackers to cause a denial of service (application crash) via vectors involving too many exceptions, which trigger a buffer overflow.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3571
5808	CVE-2016-10066	MEDIUM	Medium	Buffer overflow in the ReadVIFFImage function in coders/viff.c in ImageMagick before 6.9.4-5 allows remote attackers to cause a denial of service (application crash) via a crafted file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3545
5809	CVE-2016-10065	MEDIUM	High	The ReadVIFFImage function in coders/viff.c in ImageMagick before 7.0.1-0 allows remote attackers to cause a denial of service (application crash) or other unspecified impact via a crafted file.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3525
5810	CVE-2016-10064	MEDIUM	High	Buffer overflow in coders/tiff.c in ImageMagick before 6.9.5-1 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3556
5811	CVE-2016-10063	MEDIUM	High	Buffer overflow in coders/tiff.c in ImageMagick before 6.9.5-1 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file, related to extend validity.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3552
5812	CVE-2016-10062	MEDIUM	Medium	The ReadGROUP4Image function in coders/tiff.c in ImageMagick does not check the return value of the fwrite function, which allows remote attackers to cause a denial of service (application crash) via a crafted file.	imagemagick	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3501
5813	CVE-2016-10061	MEDIUM	Medium	The ReadGROUP4Image function in coders/tiff.c in ImageMagick before 7.0.1-10 does not check the return value of the fputc function, which allows remote attackers to cause a denial of service (crash) via a crafted image file.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3499
5814	CVE-2016-10060	MEDIUM	Medium	The ConcatenateImages function in MagickWand/magick-cli.c in ImageMagick before 7.0.1-10 does not check the return value of the fputc function, which allows remote attackers to cause a denial of service (application crash) via a crafted file.	imagemagick	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3574
5815	CVE-2016-10059	MEDIUM	High	Buffer overflow in coders/tiff.c in ImageMagick before 6.9.4-1 allows remote attackers to cause a denial of service (application crash) or have unspecified other impact via a crafted TIFF file.	imagemagick	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3772
5816	CVE-2016-10058	HIGH	Medium	Memory leak in the ReadPSDLayers function in coders/psd.c in ImageMagick before 6.9.6-3 allows remote attackers to cause a denial of service (memory consumption) via a crafted image file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3718
5817	CVE-2016-10057	MEDIUM	High	Buffer overflow in the WriteGROUP4Image function in coders/tiff.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3814
5818	CVE-2016-10056	MEDIUM	High	Buffer overflow in the sixel_decode function in coders/sixel.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3713

	A	B	C	D	E	F	G	H	I	J	K	L	M
5819	CVE-2016-10055	MEDIUM	High	Buffer overflow in the WritePDBImage function in coders/pdb.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3778
5820	CVE-2016-10054	MEDIUM	High	Buffer overflow in the WriteMAPImage function in coders/map.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3786
5821	CVE-2016-10053	MEDIUM	Medium	The WriteTIFFImage function in coders/tiff.c in ImageMagick before 6.9.5-8 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3681
5822	CVE-2016-10052	MEDIUM	High	Buffer overflow in the WriteProfile function in coders/jpeg.c in ImageMagick before 6.9.5-6 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3761
5823	CVE-2016-10051	MEDIUM	High	Use-after-free vulnerability in the ReadPWPImage function in coders/pwp.c in ImageMagick 6.9.5-5 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3703
5824	CVE-2016-10050	MEDIUM	High	Heap-based buffer overflow in the ReadRLEImage function in coders/rle.c in ImageMagick 6.9.4-8 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted RLE file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3810
5825	CVE-2016-10049	MEDIUM	High	Buffer overflow in the ReadRLEImage function in coders/rle.c in ImageMagick before 6.9.4-4 allows remote attackers to cause a denial of service (application crash) or have other unspecified impact via a crafted RLE file.	imagemagick	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3702
5826	CVE-2016-10048	MEDIUM	High	Directory traversal vulnerability in magick/module.c in ImageMagick 6.9.4-7 allows remote attackers to load arbitrary modules via unspecified vectors.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3802
5827	CVE-2016-10047	HIGH	Medium	Memory leak in the NewXMLTree function in magick/xml-tree.c in ImageMagick before 6.9.4-7 allows remote attackers to cause a denial of service (memory consumption) via a crafted XML file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3637
5828	CVE-2016-10046	MEDIUM	Medium	Heap-based buffer overflow in the DrawImage function in magick/draw.c in ImageMagick before 6.9.5-5 allows remote attackers to cause a denial of service (application crash) via a crafted image file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3801
5829	CVE-2016-10044	HIGH	High	The aio_mount function in fs/aio.c in the Linux kernel before 4.7.7 does not properly restrict execute access, which makes it easier for local users to bypass intended SELinux W^X policy restrictions, and consequently gain privileges, via an io_setup system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3255
5830	CVE-2016-10040	MEDIUM	Medium	Stack-based buffer overflow in QXmlSimpleReader in Qt 4.8.5 allows remote attackers to cause a denial of service (application crash) via a xml file with multiple nested open tags.	qt	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-3538
5831	CVE-2016-10029	LOW	Medium	The virtio_gpu_set_scanout function in QEMU (aka Quick Emulator) built with Virtio GPU Device emulator support allows local guest OS users to cause a denial of service (out-of-bounds read and process crash) via a scanout id in a VIRTIO_GPU_CMD_SET_SCANOUT command larger than num_scanouts.	qemu	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3544
5832	CVE-2016-10028	LOW	Medium	The virgl_cmd_get_capset function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) built with Virtio GPU Device emulator support allows local guest OS users to cause a denial of service (out-of-bounds read and process crash) via a VIRTIO_GPU_CMD_GET_CAPSET command with a maximum capabilities size with a value of 0.	qemu	Unchanged	Not vulnerable	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3505
5833	CVE-2016-10012	HIGH	High	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.	openssh	Unchanged	8.0.0.13	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2925
5834	CVE-2016-10011	LOW	Medium	authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.	openssh	Unchanged	8.0.0.13	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2924
5835	CVE-2016-10010	MEDIUM	High	sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.	openssh	Unchanged	8.0.0.14	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2952
5836	CVE-2016-10009	HIGH	High	Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.	openssh	Unchanged	8.0.0.13	9.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2923

	A	B	C	D	E	F	G	H	I	J	K	L	M
5837	CVE-2016-1000110	MEDIUM	MEDIUM	Find out more about CVE-2016-1000110 from the MITRE CVE dictionary dictionary and NIST NVD. CVSS v2 metrics NOTE: The following CVSS v2 metrics and score provided are preliminary and subject to review. Base Score 5 Base Metrics AV:N/AC:L/Au:N/C:N/I:P/A:N Access Vector Network Access Complexity Low Authentication None Confidentiality Impact None Integrity Impact Partial Availability Impact None CVSS v3 metrics NOTE: The following CVSS v3 metrics and score provided are preliminary and subject to review. CVSS3 Base Score 5 CVSS3 Base Metrics CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N Attack Vector Network Attack Complexity Low Privileges Required Low User Interaction None Scope Changed Confidentiality None Integrity Impact Low Availability Impact None Find out more about Red Hat support for the Common Vulnerability Scoring System (CVSS). Affected Packages State Platform Package State Red Hat Enterprise Linux 7 python Affected Red Hat Enterprise Linux 4 python Will not fix Red Hat Enterprise Linux 5 python Affected Red Hat Enterprise Linux 6 python Affected Acknowledgements Red Hat would like to thank Scott Geary (VendHQ) for reporting this issue. This page is generated automatically and has not been checked for errors or omissions. For clarification or corrections please contact Red Hat Product Security. Last Modified July 27 2016 at 2:32 PM	python	Unchanged	8.0.0.9	unknown	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1393
5838	CVE-2016-1000030	HIGH	CRITICAL	Pidgin version <2.11.0 contains a vulnerability in X.509 Certificates imports specifically due to improper check of return values from gnutls_x509_crt_init() and gnutls_x509_crt_import() that can result in code execution. This attack appear to be exploitable via custom X.509 certificate from another client. This vulnerability appears to have been fixed in 2.11.0.	pidgin	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-4728
5839	CVE-2016-0823	LOW	Medium	The pagemap_open function in fs/proc/task_mmu.c in the Linux kernel before 3.19.3, as used in Android 6.0.1 before 2016-03-01, allows local users to obtain sensitive physical-address information by reading a pagemap file, aka Android internal bug 25739721.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-365
5840	CVE-2016-0821	MEDIUM	High	The LIST_POISON feature in include/linux/poison.h in the Linux kernel before 4.3, as used in Android 6.0.1 before 2016-03-01, does not properly consider the relationship to the mmap_min_addr value, which makes it easier for attackers to bypass a poison-pointer protection mechanism by triggering the use of an uninitialized list entry, aka Android internal bug 26186802, a different vulnerability than CVE-2015-3636.	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-358
5841	CVE-2016-0800	MEDIUM	Medium	The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a DROWN attack.	openssl	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-323
5842	CVE-2016-0799	HIGH	Critical	The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842.	openssl	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-327
5843	CVE-2016-0798	HIGH	High	Memory leak in the SRP_VBASE_get_by_user implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt, related to apps/s_server.c and crypto/srp/srp_vfy.c.	openssl	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-325
5844	CVE-2016-0797	MEDIUM	High	Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference) or possibly have unspecified other impact via a long digit string that is mishandled by the (1) BN_dec2bn or (2) BN_hex2bn function, related to crypto/bn/bn.h and crypto/bn/bn_print.c.CWE-190: Integer Overflow or Wraparound CWE-476: NULL Pointer Dereference	openssl	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-326
5845	CVE-2016-0787	MEDIUM	Medium	The diffie_hellman_sha256 function in kex.c in libssh2 before 1.7.0 improperly truncates secrets to 128 or 256 bits, which makes it easier for man-in-the-middle attackers to decrypt or intercept SSH sessions via unspecified vectors, aka a bits/bytes confusion bug.	libssh2	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-457
5846	CVE-2016-0778	MEDIUM	High	The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.	openssh	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-143
5847	CVE-2016-0777	MEDIUM	Medium	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.	openssh	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-142

	A	B	C	D	E	F	G	H	I	J	K	L	M
5848	CVE-2016-0774	MEDIUM	Medium	The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in a certain Linux kernel backport in the linux package before 3.2.73-2+deb7u3 on Debian wheezy and the kernel package before 3.10.0-229.26.2 on Red Hat Enterprise Linux (RHEL) 7.1 do not properly consider the side effects of failed __copy_to_user_inatomic and __copy_from_user_inatomic calls, which allows local users to cause a denial of service (system crash) or possibly gain privileges via a crafted application, aka an I/O vector array overrun. NOTE: this vulnerability exists because of an incorrect fix for CVE-2015-1805.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-666
5849	CVE-2016-0773	MEDIUM	High	PostgreSQL before 9.1.20, 9.2.x before 9.2.15, 9.3.x before 9.3.11, 9.4.x before 9.4.6, and 9.5.x before 9.5.1 allows remote attackers to cause a denial of service (infinite loop or buffer overflow and crash) via a large Unicode character range in a regular expression.	postgresql	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-301
5850	CVE-2016-0772	MEDIUM	Medium	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a StartTLS stripping attack.	python	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1559
5851	CVE-2016-0771	MEDIUM	Medium	The internal DNS server in Samba 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6, and 4.4.x before 4.4.0rc4, when an AD DC is configured, allows remote authenticated users to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from process memory by uploading a crafted DNS TXT record.	samba	Unchanged	8.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-401
5852	CVE-2016-0766	HIGH	High	PostgreSQL before 9.1.20, 9.2.x before 9.2.15, 9.3.x before 9.3.11, 9.4.x before 9.4.6, and 9.5.x before 9.5.1 does not properly restrict access to unspecified custom configuration settings (GUCS) for PL/Java, which allows attackers to gain privileges via unspecified vectors.	postgresql	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-319
5853	CVE-2016-0758	HIGH	High	Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data.CWE-190: Integer Overflow or Wraparound	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-932
5854	CVE-2016-0755	MEDIUM	High	The ConnectionExists function in lib/url.c in libcurl before 7.47.0 does not properly re-use NTLM-authenticated proxy connections, which might allow remote attackers to authenticate as other users via a request, a similar issue to CVE-2014-0015.	curl	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-234
5855	CVE-2016-0754	MEDIUM	Medium	cURL before 7.47.0 on Windows allows attackers to write to arbitrary files in the current working directory on a different drive via a colon in a remote file name.	curl	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-249
5856	CVE-2016-0747	MEDIUM	Medium	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 does not properly limit CNAME resolution, which allows remote attackers to cause a denial of service (worker process resource consumption) via vectors related to arbitrary name resolution.	nginx	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-304
5857	CVE-2016-0746	HIGH	High	Use-after-free vulnerability in the resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (worker process crash) or possibly have unspecified other impact via a crafted DNS response related to CNAME response processing.	nginx	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-294
5858	CVE-2016-0742	MEDIUM	Medium	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (invalid pointer dereference and worker process crash) via a crafted UDP DNS response.	nginx	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-305
5859	CVE-2016-0739	MEDIUM	Medium	libssh before 0.7.3 improperly truncates ephemeral secrets generated for the (1) diffie-hellman-group1 and (2) diffie-hellman-group14 key exchange methods to 128 bits, which makes it easier for man-in-the-middle attackers to decrypt or intercept SSH sessions via unspecified vectors, aka a bits/bytes confusion bug.	libssh	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-494
5860	CVE-2016-0736	MEDIUM	High	It was discovered that the mod_session_crypto module of httpd did not use any mechanisms to verify integrity of the encrypted session data stored in the user's browser. A remote attacker could use this flaw to decrypt and modify session data using a padding oracle attack.	apache	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3985
5861	CVE-2016-0729	HIGH	Critical	Multiple buffer overflows in (1) internal/XMLReader.cpp, (2) util/XMLURL.cpp, and (3) util/XMLUri.cpp in the XML Parser library in Apache Xerces-C before 3.1.3 allow remote attackers to cause a denial of service (segmentation fault or memory corruption) or possibly execute arbitrary code via a crafted document.	xerces-c	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-441
5862	CVE-2016-0728	HIGH	High	A use-after-free flaw was found in the way the Linux kernel's key management subsystem handled keyring object reference counting in certain error path of the join_session_keyring() function. A local, unprivileged user could use this flaw to escalate their privileges on the system.	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-153
5863	CVE-2016-0727	HIGH	High	Multiple bugs in cronjob script bundled with ntp package were found allowing malicious ntp user to make the backup process to overwrite arbitrary files with content controlled by the attacker, thus gaining root privileges.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3838
5864	CVE-2016-0723	MEDIUM	Medium	Race condition in the tty_ioctl function in drivers/tty/tty_io.c in the Linux kernel through 4.4.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (use-after-free and system crash) by making a TIOCGETD ioctl call during processing of a TIOCSETD ioctl call.	linux	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-250

	A	B	C	D	E	F	G	H	I	J	K	L	M
5865	CVE-2016-0718	HIGH	Critical	Expat allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a malformed input document, which triggers a buffer overflow.	expat	Unchanged	8.0.0.8	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-729
5866	CVE-2016-0705	HIGH	Critical	Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key.CWE-415: Double Free	openssl	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-324
5867	CVE-2016-0704	MEDIUM	Medium	An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-330
5868	CVE-2016-0703	MEDIUM	Medium	The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-329
5869	CVE-2016-0702	LOW	Medium	The MOD_EXP_CTIME_COPY_FROM_PREBUF function in crypto/bn/bn_exp.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not properly consider cache-bank access times during modular exponentiation, which makes it easier for local users to discover RSA keys by running a crafted application on the same Intel Sandy Bridge CPU core as a victim and leveraging cache-bank conflicts, aka a CacheBleed attack.	openssl	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-328
5870	CVE-2016-0701	LOW	Low	It was found that OpenSSL used weak Diffie-Hellman parameters based on unsafe primes, which were generated and stored in X9.42-style parameter files. An attacker who could force the peer to perform multiple handshakes using the same private DH component could use this flaw to conduct man-in-the-middle attacks on the SSL/TLS connection.	openssl	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-240
5871	CVE-2016-0668	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.6.28 and earlier and 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-467
5872	CVE-2016-0667	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Locking.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-519
5873	CVE-2016-0666	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect availability via vectors related to Security: Privileges.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-499
5874	CVE-2016-0665	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.6.28 and earlier and 5.7.10 and earlier allows local users to affect availability via vectors related to Security: Encryption.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-469
5875	CVE-2016-0663	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to Performance Schema.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-518
5876	CVE-2016-0662	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-463
5877	CVE-2016-0661	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.6.28 and earlier and 5.7.10 and earlier allows local users to affect availability via vectors related to Options.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-502
5878	CVE-2016-0659	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-470
5879	CVE-2016-0658	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-511
5880	CVE-2016-0657	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect confidentiality via vectors related to JSON.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-464
5881	CVE-2016-0656	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB, a different vulnerability than CVE-2016-0654.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-505
5882	CVE-2016-0655	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.6.29 and earlier and 5.7.11 and earlier allows local users to affect availability via vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-508
5883	CVE-2016-0654	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB, a different vulnerability than CVE-2016-0656.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-483
5884	CVE-2016-0653	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to FTS.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-500
5885	CVE-2016-0652	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-471
5886	CVE-2016-0651	LOW	Medium	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier allows local users to affect availability via vectors related to Optimizer.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-478
5887	CVE-2016-0650	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to Replication.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-520
5888	CVE-2016-0649	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to PS.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-490

	A	B	C	D	E	F	G	H	I	J	K	L	M
5889	CVE-2016-0648	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect availability via vectors related to PS.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-513
5890	CVE-2016-0647	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect availability via vectors related to FTS.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-517
5891	CVE-2016-0646	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to DML.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-474
5892	CVE-2016-0644	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect availability via vectors related to DDL.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-497
5893	CVE-2016-0643	MEDIUM	Low	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect confidentiality via vectors related to DML.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-465
5894	CVE-2016-0642	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect integrity and availability via vectors related to Federated.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-522
5895	CVE-2016-0641	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect confidentiality and availability via vectors related to MyISAM.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-480
5896	CVE-2016-0640	MEDIUM	Medium	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier allows local users to affect integrity and availability via vectors related to DML.	mysql	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-461
5897	CVE-2016-0639	HIGH	Critical	Unspecified vulnerability in Oracle MySQL 5.6.29 and earlier and 5.7.11 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Pluggable Authentication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-486
5898	CVE-2016-0634	MEDIUM	High	A vulnerability was found in a way bash expands the $HOSTNAME. Injecting the hostname with malicious code would cause it to run each time bash expanded \h in the prompt string.	bash	Unchanged	8.0.0.17	9.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3955
5899	CVE-2016-0616	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-171
5900	CVE-2016-0611	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-182
5901	CVE-2016-0610	LOW		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-188
5902	CVE-2016-0609	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to privileges.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-185
5903	CVE-2016-0608	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via vectors related to UDF.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-183
5904	CVE-2016-0607	LOW		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to replication.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-184
5905	CVE-2016-0606	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect integrity via unknown vectors related to encryption.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-180
5906	CVE-2016-0605	LOW		Unspecified vulnerability in Oracle MySQL 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-176
5907	CVE-2016-0601	LOW		Unspecified vulnerability in Oracle MySQL 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Partition.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-201
5908	CVE-2016-0600	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-163
5909	CVE-2016-0599	LOW		Unspecified vulnerability in Oracle MySQL 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-155
5910	CVE-2016-0598	LOW		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-178
5911	CVE-2016-0597	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-170
5912	CVE-2016-0596	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier and 5.6.27 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-191
5913	CVE-2016-0595	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-157
5914	CVE-2016-0594	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.21 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-203
5915	CVE-2016-0546	HIGH		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Client.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-162
5916	CVE-2016-0505	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Options.	mysql	Updated	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-164

	A	B	C	D	E	F	G	H	I	J	K	L	M
5917	CVE-2016-0504	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0503.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-172
5918	CVE-2016-0503	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0504.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-206
5919	CVE-2016-0502	MEDIUM		Unspecified vulnerability in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Updated	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-158
5920	CVE-2015-9383	Medium	MEDIUM	FreeType before 2.6.2 has a heap-based buffer over-read in tt_cmap14_validate in sfnt/ttcmap.c.	freetype	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4829
5921	CVE-2015-9382	Medium	MEDIUM	FreeType before 2.6.1 has a buffer over-read in skip_comment in psaux/psobjs.c because ps_parser_skip_PS_token is mishandled in an FT_New_Memory_Face operation.	freetype	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4830
5922	CVE-2015-9381	Medium	HIGH	FreeType before 2.6.1 has a heap-based buffer over-read in T1_Get_Private_Dict in type1/t1parse.c.	freetype	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4831
5923	CVE-2015-9290			In FreeType before 2.6.1, a buffer over-read occurs in type1/t1parse.c on function T1_Get_Private_Dict where there is no check that the new values of cur and limit are sensible before going to Again.	freetype	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4572
5924	CVE-2015-9289			In the Linux kernel before 4.1.4, a buffer overflow occurs when checking userspace params in drivers/media/dvb-frontends/cx24116.c. The maximum size for a DiSEqC command is 6, according to the userspace API. However, the code allows larger values such as 23.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4547
5925	CVE-2015-9274			HarfBuzz before 1.0.4 allows remote attackers to cause a denial of service (invalid read of two bytes and application crash) because of GPOS and GSUB table mishandling, related to hb-ot-layout-gpos-table.hh, hb-ot-layout-gsub-table.hh, and hb-ot-layout-gsubgpos-private.hh.	harfbuzz	Unchanged	8.0.0.28	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4984
5926	CVE-2015-9262			_XcursorThemeInherits in library.c in libXcursor before 1.1.15 allows remote attackers to cause denial of service or potentially code execution via a one-byte heap overflow.	libxcursor	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4538
5927	CVE-2015-9261			huft_build in archival/libarchive/decompress_gunzip.c in BusyBox before 1.27.2 misuses a pointer, causing segfaults and an application crash during an unzip operation on a specially crafted ZIP file.	busybox	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4418
5928	CVE-2015-9253			An issue was discovered in PHP through 7.2.2. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.	php	Unchanged	8.0.0.27	9.0.0.18	10.17.41.11	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3360
5929	CVE-2015-9101	MEDIUM	Medium	The fill_buffer_resample function in util.c in libmp3lame.a in LAME 3.99.5 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted audio file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4570
5930	CVE-2015-9100	MEDIUM	Medium	The fill_buffer_resample function in util.c in libmp3lame.a in LAME 3.99.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted audio file.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4532
5931	CVE-2015-9099	MEDIUM	Medium	The lame_init_params function in lame.c in libmp3lame.a in LAME 3.99.5 allows remote attackers to cause a denial of service (invalid read and application crash) via a crafted audio file with a negative sample rate.	lame	Unchanged	8.0.0.28	9.0.0.19	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4558
5932	CVE-2015-9096	MEDIUM	Medium	Net::SMTP in Ruby before 2.4.0 is vulnerable to SMTP command injection via CRLF sequences in a RCPT TO or MAIL FROM command, as demonstrated by CRLF sequences immediately before and after a DATA substring.	ruby	Unchanged	8.0.0.19	9.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4393
5933	CVE-2015-9059	High	Critical	picocom before 2.0 has a command injection vulnerability in the 'send and receive file' command because the command line is executed by /bin/sh unsafely.	picocom	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4413
5934	CVE-2015-9019	MEDIUM	Medium	In libxslt 1.1.29 and earlier, the EXSLT math.random function was not initialized with a random seed during startup, which could cause usage of this function to produce predictable outputs.	libxslt	Unchanged	Vulnerable	Vulnerable	Investigate	Investigate	Investigate	Not vulnerable	LIN9-3886
5935	CVE-2015-9016			In blk_mq_tag_to_rq in blk-mq.c in the upstream kernel, there is a possible use after free due to a race condition when a request has been previously freed by blk_mq_complete_request. This could lead to local escalation of privilege. Product: Android. Versions: Android kernel. Android ID: A-63083046.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3760
5936	CVE-2015-9004	High	High	kernel/events/core.c in the Linux kernel before 3.19 mishandles counter grouping, which allows local users to gain privileges via a crafted application, related to the perf_pmu_register and perf_event_open functions.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4235

	A	B	C	D	E	F	G	H	I	J	K	L	M
5937	CVE-2015-8994	MEDIUM	High	An issue was discovered in PHP 5.x and 7.x, when the configuration uses apache2handler/mod_php or php-fpm with OpCache enabled. With 5.x after 5.6.28 or 7.x after 7.0.13, the issue is resolved in a non-default configuration with the opcache.validate_permission=1 setting. The vulnerability details are as follows. In PHP SAPIs where PHP interpreters share a common parent process, Zend OpCache creates a shared memory object owned by the common parent during initialization. Child PHP processes inherit the SHM descriptor, using it to cache and retrieve compiled script bytecode (opcode in PHP jargon). Cache keys vary depending on configuration, but filename is a central key component, and compiled opcode can generally be run if a script's filename is known or can be guessed. Many common shared-hosting configurations change EUID in child processes to enforce privilege separation among hosted users (for example using mod_ruid2 for the Apache HTTP Server, or php-fpm user settings). In these scenarios, the default Zend OpCache behavior defeats script file permissions by sharing a single SHM cache among all child PHP processes. PHP scripts often contain sensitive information: Think of CMS configurations where reading or running another user's script usually means gaining privileges to the CMS database.	php	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3559
5938	CVE-2015-8985	Medium	Medium	The pop_fail_stack function in the GNU C Library (aka glibc or libc6) allows context-dependent attackers to cause a denial of service (assertion failure and application crash) via vectors related to extended regular expression processing.	glibc	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN9-3731
5939	CVE-2015-8984	Medium	Medium	The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (application crash) via a malformed pattern, which triggers an out-of-bounds read.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3745
5940	CVE-2015-8983	Medium	High	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a size in bytes, which triggers a heap-based buffer overflow.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3784
5941	CVE-2015-8982	Medium	High	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3707
5942	CVE-2015-8971	Medium	High	Terminology 0.7.0 allows remote attackers to execute arbitrary commands via escape sequences that modify the window title and then are written to the terminal, a similar issue to CVE-2003-0063.	terminology	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3305
5943	CVE-2015-8970	Medium	Medium	crypto/algif_skcipher.c in the Linux kernel before 4.4.2 does not verify that a setkey operation has been performed on an AF_ALG socket before an accept system call is processed, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted application that does not supply a key, related to the lrw_crypt function in crypto/lrw.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2797
5944	CVE-2015-8967	High	High	arch/arm64/kernel/sys.c in the Linux kernel before 4.0 allows local users to bypass the strict page permissions protection mechanism and modify the system-call table, and consequently gain privileges, by leveraging write access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2780
5945	CVE-2015-8966	High	High	arch/arm/kernel/sys_oabi-compat.c in the Linux kernel before 4.4 allows local users to gain privileges via a crafted (1) F_OFD_GETLK, (2) F_OFD_SETLK, or (3) F_OFD_SETLKW command in an fcntl64 system call.	linux	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2790
5946	CVE-2015-8964	High	Medium	The tty_set_termios_ldisc function in drivers/tty/tty_ldisc.c in the Linux kernel before 4.5 allows local users to obtain sensitive information from kernel memory by reading a tty data structure.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2280
5947	CVE-2015-8963	High	High	Race condition in kernel/events/core.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging incorrect handling of an swevent data structure during a CPU unplug operation.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2403
5948	CVE-2015-8962	High	High	Double free vulnerability in the sg_common_write function in drivers/scsi/sg.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (memory corruption and system crash) by detaching a device during an SG_IO ioctl call.	linux	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2266
5949	CVE-2015-8961	High	High	The __ext4_journal_stop function in fs/ext4/ext4_jbd2.c in the Linux kernel before 4.3.3 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging improper access to a certain error field.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2267
5950	CVE-2015-8959	HIGH	Medium	coders/dds.c in ImageMagick before 6.9.0-4 Beta allows remote attackers to cause a denial of service (CPU consumption) via a crafted DDS file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4089
5951	CVE-2015-8958	MEDIUM	Medium	coders/sun.c in ImageMagick before 6.9.0-4 Beta allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted SUN file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4140
5952	CVE-2015-8957	MEDIUM	Medium	Buffer overflow in ImageMagick before 6.9.0-4 Beta allows remote attackers to cause a denial of service (application crash) via a crafted SUN file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4029
5953	CVE-2015-8956	Low	Medium	The rfcomm_sock_bind function in net/bluetooth/rfcomm/sock.c in the Linux kernel before 4.2 allows local users to obtain sensitive information or cause a denial of service (NULL pointer dereference) via vectors involving a bind system call on a Bluetooth RFCOMM socket.	linux	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1734

	A	B	C	D	E	F	G	H	I	J	K	L	M
5954	CVE-2015-8955	Medium	High	arch/arm64/kernel/perf_event.c in the Linux kernel before 4.1 on arm64 platforms allows local users to gain privileges or cause a denial of service (invalid pointer dereference) via vectors involving events that are mishandled during a span of multiple HW PMUs.	linux	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1731
5955	CVE-2015-8954	High	Critical	The MemcmpLowercase function in Suricata before 2.0.6 improperly excludes the first byte from comparisons, which might allow remote attackers to bypass intrusion-prevention functionality via a crafted HTTP request.	suricata	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3771
5956	CVE-2015-8953	Medium	Medium	fs/overlayfs/copy_up.c in the Linux kernel before 4.2.6 uses an incorrect cleanup code path, which allows local users to cause a denial of service (dentry reference leak) via filesystem operations on a large file in a lower overlayfs layer.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1829
5957	CVE-2015-8952	Low	Medium	The mbcache feature in the ext2 and ext4 filesystem implementations in the Linux kernel before 4.6 mishandles xattr block caching, which allows local users to cause a denial of service (soft lockup) via filesystem operations in environments that use many attributes, as demonstrated by Ceph and Samba.	linux	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1838
5958	CVE-2015-8950	Medium	Medium	arch/arm64/mm/dma-mapping.c in the Linux kernel before 4.0.3, as used in the ION subsystem in Android and other products, does not initialize certain data structures, which allows local users to obtain sensitive information from kernel memory by triggering a dma_mmap call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1752
5959	CVE-2015-8948	Medium	High	idn in GNU libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read.	libidn	Unchanged	8.0.0.10	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1564
5960	CVE-2015-8947	High	High	hb-ot-layout-gpos-table.hh in HarfBuzz before 1.0.5 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted data, a different vulnerability than CVE-2016-2052.	harfbuzz	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1299
5961	CVE-2015-8946	LOW	Low	ecryptfs-setup-swap in eCryptfs before 111 does not prevent the unencrypted swap partition from activating during boot when using GPT partitioning and certain versions of systemd, which allows local users to obtain sensitive information via unspecified vectors.	ecryptfs-utils	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1287
5962	CVE-2015-8944	Medium	Medium	The ioresources_init function in kernel/resource.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 6 and 7 (2013) devices, uses weak permissions for /proc/iomem, which allows local users to obtain sensitive information by reading this file, aka Android internal bug 28814213 and Qualcomm internal bug CR786116. NOTE: the permissions may be intentional in most non-Android contexts.	linux	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1390
5963	CVE-2015-8935	Medium	Medium	The sapi_header_op function in main/SAPI.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 supports deprecated line folding without considering browser compatibility, which allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging (1) %0A %20 or (2) %0D%0A%20 mishandling in the header function.	php	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1362
5964	CVE-2015-8934	Medium	Medium	The copy_from_lzss_window function in archive_read_support_format_rar.c in libarchive 3.2.0 and earlier allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted rar file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1631
5965	CVE-2015-8933	Medium	Medium	Integer overflow in the archive_read_format_tar_skip function in archive_read_support_format_tar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted tar file.	libarchive	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1639
5966	CVE-2015-8932	Medium	Medium	The compress_bidder_init function in archive_read_support_filter_compress.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted tar file, which triggers an invalid left shift.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1636
5967	CVE-2015-8931	Medium	High	Multiple integer overflows in the (1) get_time_t_max and (2) get_time_t_min functions in archive_read_support_format_mtree.c in libarchive before 3.2.0 allow remote attackers to have unspecified impact via a crafted mtree file, which triggers undefined behavior.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1634
5968	CVE-2015-8930	Medium	High	bsdtar in libarchive before 3.2.0 allows remote attackers to cause a denial of service (infinite loop) via an ISO with a directory that is a member of itself.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1617
5969	CVE-2015-8929	Medium	Medium	Memory leak in the __archive_read_get_extract function in archive_read_extract2.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service via a tar file.	libarchive	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1619
5970	CVE-2015-8928	Medium	Medium	The process_add_entry function in archive_read_support_format_mtree.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mtree file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1638
5971	CVE-2015-8927	Medium	Medium	The trad_enc_decrypt_update function in archive_read_support_format_zip.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds heap read and crash) via a crafted zip file, related to reading the password.	libarchive	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1616
5972	CVE-2015-8926	Medium	Medium	The archive_read_format_rar_read_data function in archive_read_support_format_rar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted rar archive.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1618
5973	CVE-2015-8925	Medium	Medium	The readline function in archive_read_support_format_mtree.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (invalid read) via a crafted mtree file, related to newline parsing.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1625
5974	CVE-2015-8924	Medium	Medium	The archive_read_format_tar_read_header function in archive_read_support_format_tar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tar file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1626

	A	B	C	D	E	F	G	H	I	J	K	L	M
5975	CVE-2015-8923	Medium	Medium	The process_extra function in libarchive before 3.2.0 uses the size field and a signed number in an offset, which allows remote attackers to cause a denial of service (crash) via a crafted zip file.	libarchive	Unchanged	8.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1612
5976	CVE-2015-8922	Medium	Medium	The read_CodersInfo cuntion in archive_read_support_format_7zip.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (NULL pointer derference and crash) via a crafted 7z file, related to the _7z_folder struct.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1615
5977	CVE-2015-8921	Medium	High	The ae_strtofflags function in archive_entry.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mtree file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1609
5978	CVE-2015-8920	Medium	Medium	The _ar_read_header function in archive_read_support_format_ar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds stack read) via a crafted ar file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1637
5979	CVE-2015-8919	Medium	High	The lha_read_file_extended_header function in archive_read_support_format_lha.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds heap) via a crafted (1) lzh or (2) lha file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1607
5980	CVE-2015-8918	Medium	High	The archive_string_append function in archive_string.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted cab files, related to overlapping memcpy.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1640
5981	CVE-2015-8917	Medium	High	bsdtar in libarchive before 3.2.0 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via an invalid character in the name of a cab file.	libarchive	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1611
5982	CVE-2015-8916	Medium	Medium	bsdtar in libarchive before 3.2.0 returns a success code without filling the entry when the header is a split file in multivolume RAR, which allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted rar file.	libarchive	Unchanged	8.0.0.12	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1623
5983	CVE-2015-8915	Medium	Medium	bsdcpio in libarchive before 3.2.0 allows remote attackers to cause a denial of service (invalid read and crash) via crafted cpio file.	libarchive	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1606
5984	CVE-2015-8903	Medium	Medium	The ReadVICARImage function in coders/vicar.c in ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted VICAR file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3506
5985	CVE-2015-8902	Medium	Medium	The ReadBlobByte function in coders/pdb.c in ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted PDB file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3553
5986	CVE-2015-8901	Medium	Medium	ImageMagick 6.x before 6.9.0-5 Beta allows remote attackers to cause a denial of service (infinite loop) via a crafted MIFF file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3585
5987	CVE-2015-8900	Medium	Medium	The ReadHDRImage function in coders/hdr.c in ImageMagick 6.x and 7.x allows remote attackers to cause a denial of service (infinite loop) via a crafted HDR file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3514
5988	CVE-2015-8899	Medium	High	Dnsmasq before 2.76 allows remote servers to cause a denial of service (crash) via a reply with an empty DNS address that has an (1) A or (2) AAAA record defined locally.	dnsmasq	Unchanged	8.0.0.11	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1112
5989	CVE-2015-8898	Medium	Medium	The WriteImages function in magick/constitute.c in ImageMagick before 6.9.2-4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted image file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3759
5990	CVE-2015-8897	Medium	Medium	The SpliceImage function in MagickCore/transform.c in ImageMagick before 6.9.2-4 allows remote attackers to cause a denial of service (application crash) via a crafted png file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3768
5991	CVE-2015-8896	Medium	Medium	Integer truncation issue in coders/pict.c in ImageMagick before 7.0.5-0 allows remote attackers to cause a denial of service (application crash) via a crafted .pict file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3805
5992	CVE-2015-8895	Medium	High	Integer overflow in coders/icon.c in ImageMagick 6.9.1-3 and later allows remote attackers to cause a denial of service (application crash) via a crafted length value, which triggers a buffer overflow.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3653
5993	CVE-2015-8894	Medium	Medium	Double free vulnerability in coders/tga.c in ImageMagick 7.0.0 and later allows remote attackers to cause a denial of service (application crash) via a crafted tga file.	imagemagick	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3680
5994	CVE-2015-8880	High	Critical	Double free vulnerability in the format printer in PHP 7.x before 7.0.1 allows remote attackers to have an unspecified impact by triggering an error.CWE-415: Double Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-728
5995	CVE-2015-8879	Medium	High	The odbc_bindcols function in ext/odbc/php_odbc.c in PHP before 5.6.12 mishandles driver behavior for SQL_WVARCHAR columns, which allows remote attackers to cause a denial of service (application crash) in opportunistic circumstances by leveraging use of the odbc_fetch_array function to access a certain type of Microsoft SQL Server table.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-723
5996	CVE-2015-8878	High	Medium	main/php_open_temporary_file.c in PHP before 5.5.28 and 5.6.x before 5.6.12 does not ensure thread safety, which allows remote attackers to cause a denial of service (race condition and heap memory corruption) by leveraging an application that performs many temporary-file accesses.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-736
5997	CVE-2015-8877	Medium	High	The gdImageScaleTwoPass function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in PHP before 5.6.12, uses inconsistent allocate and free approaches, which allows remote attackers to cause a denial of service (memory consumption) via a crafted call, as demonstrated by a call to the PHP imagescale function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-743

	A	B	C	D	E	F	G	H	I	J	K	L	M
5998	CVE-2015-8876	High	Critical	Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not validate certain Exception objects, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution via crafted serialized data.CWE-476: NULL Pointer Dereference	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-753
5999	CVE-2015-8875	Medium	High	Multiple integer overflows in the (1) pixops_composite_nearest, (2) pixops_composite_color_nearest, and (3) pixops_process functions in pixops/pixops.c in gdk-pixbuf before 2.33.1 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted image, which triggers a heap-based buffer overflow.	gdk-pixbuf	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-819
6000	CVE-2015-8874	Medium	High	Stack consumption vulnerability in GD in PHP before 5.6.12 allows remote attackers to cause a denial of service via a crafted imagefilltoborder call.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-788
6001	CVE-2015-8873	Medium	High	Stack consumption vulnerability in Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to cause a denial of service (segmentation fault) via recursive method calls.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-712
6002	CVE-2015-8872	Low	Medium	The set_fat function in fat.c in dosfstools before 4.0 might allow attackers to corrupt a FAT12 filesystem or cause a denial of service (invalid memory read and crash) by writing an odd number of clusters to the third to last entry on a FAT12 filesystem, which triggers an off-by-two error.	dosfstools	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-842
6003	CVE-2015-8870	Medium	High	Integer overflow in tools/bmp2tiff.c in LibTIFF before 4.0.4 allows remote attackers to cause a denial of service (heap-based buffer over-read), or possibly obtain sensitive information from process memory, via crafted width and length values in RLE4 or RLE8 data in a BMP file.	libtiff	Unchanged	Won't Fix	9.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2725
6004	CVE-2015-8868	High	High	Heap-based buffer overflow in the ExponentialFunction::ExponentialFunction function in Poppler before 0.40.0 allows remote attackers to cause a denial of service (memory corruption and crash) or possibly execute arbitrary code via an invalid blend mode in the ExtGState dictionary in a crafted PDF document.	poppler	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-622
6005	CVE-2015-8867	Medium	High	The openssl_random_pseudo_bytes function in ext/openssl/openssl.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 incorrectly relies on the deprecated RAND_pseudo_bytes function, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-705
6006	CVE-2015-8866	Medium	Critical	ext/libxml/libxml.c in PHP before 5.5.22 and 5.6.x before 5.6.6, when PHP-FPM is used, does not isolate each thread from libxml_disable_entity_loader changes in other threads, which allows remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks via a crafted XML document, a related issue to CVE-2015-5161.CWE-611: Improper Restriction of XML External Entity Reference ('XXE')	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-785
6007	CVE-2015-8865	High	High	The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-740
6008	CVE-2015-8863	High	Critical	Off-by-one error in the tokenadd function in jv_parse.c in jq allows remote attackers to cause a denial of service (crash) via a long JSON-encoded number, which triggers a heap-based buffer overflow.	jq	Unchanged	8.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-645
6009	CVE-2015-8853	Medium	High	The (1) S_reghop3, (2) S_reghop4, and (3) S_reghopmaybe3 functions in regexec.c in Perl before 5.24.0 allow context-dependent attackers to cause a denial of service (infinite loop) via crafted utf-8 data, as demonstrated by a\x80.	perl	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-703
6010	CVE-2015-8845	Medium	Medium	The tm_reclaim_thread function in arch/powerpc/kernel/process.c in the Linux kernel before 4.4.1 on powerpc platforms does not ensure that TM suspend mode exists before proceeding with a tm_reclaim call, which allows local users to cause a denial of service (TM Bad Thing exception and panic) via a crafted application.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-606
6011	CVE-2015-8844	Medium	Medium	The signal implementation in the Linux kernel before 4.3.5 on powerpc platforms does not check for an MSR with both the S and T bits set, which allows local users to cause a denial of service (TM Bad Thing exception and panic) via a crafted application.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-656
6012	CVE-2015-8842	LOW	Low	tmpfiles.d/systemd.conf in systemd before 229 uses weak permissions for /var/log/journal/%m/system.journal, which allows local users to obtain sensitive information by reading the file.	systemd	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-498
6013	CVE-2015-8839	Low	Medium	Multiple race conditions in the ext4 filesystem implementation in the Linux kernel before 4.5 allow local users to cause a denial of service (disk corruption) by writing to a page that is associated with a different user's file after unsynchronized hole punching and page-fault handling.	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-604
6014	CVE-2015-8838	Medium	Medium	ext/mysqlnd/mysqlnd.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 uses a client SSL option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, a related issue to CVE-2015-3152.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-789

	A	B	C	D	E	F	G	H	I	J	K	L	M
6015	CVE-2015-8835	High	Critical	The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not properly retrieve keys, which allows remote attackers to cause a denial of service (NULL pointer dereference, type confusion, and application crash) or possibly execute arbitrary code via crafted serialized data representing a numerically indexed _cookies array, related to the SoapClient::__call method in ext/soap/soap.c.CWE-476: NULL Pointer Dereference	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-721
6016	CVE-2015-8830	High	High	Integer overflow in the aio_setup_single_vector function in fs/aio.c in the Linux kernel 4.0 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. NOTE: this vulnerability exists because of a CVE-2012-6701 regression.CWE-190: Integer Overflow or Wraparound	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-654
6017	CVE-2015-8818	Low	Medium	The cpu_physical_memory_write_rom_internal function in exec.c in QEMU (aka Quick Emulator) does not properly skip MMIO regions, which allows local privileged guest users to cause a denial of service (guest crash) via unspecified vectors.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3010
6018	CVE-2015-8817	Low	Medium	QEMU (aka Quick Emulator) built to use 'address_space_translate' to map an address to a MemoryRegionSection is vulnerable to an OOB r/w access issue. It could occur while doing pci_dma_read/write calls. Affects QEMU versions >= 1.6.0 and <= 2.3.1. A privileged user inside guest could use this flaw to crash the guest instance resulting in DoS.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3012
6019	CVE-2015-8816	High	Medium	The hub_activate function in drivers/usb/core/hub.c in the Linux kernel before 4.3.5 does not properly maintain a hub-interface data structure, which allows physically proximate attackers to cause a denial of service (invalid memory access and system crash) or possibly have unspecified other impact by unplugging a USB hub device.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-661
6020	CVE-2015-8812	High	Critical	drivers/infiniband/hw/cxgb3/iwch_cm.c in the Linux kernel before 4.5 does not properly identify error conditions, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted packets.CWE-416: Use After Free	linux	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-614
6021	CVE-2015-8806	Medium	High	dict.c in libxml2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via an unexpected character immediately after the <!DOCTYPE html substring in a crafted HTML document.	libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-496
6022	CVE-2015-8805	HIGH	Critical	The ecc_256_modq function in ecc-256.c in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-256 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors, a different vulnerability than CVE-2015-8803.	nettle	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-318
6023	CVE-2015-8804	HIGH	Critical	x86_64/ecc-384-modp.asm in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-384 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors.	nettle	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-313
6024	CVE-2015-8803	HIGH	Critical	The ecc_256_modp function in ecc-256.c in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-256 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors, a different vulnerability than CVE-2015-8805.	nettle	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-310
6025	CVE-2015-8792	Medium	Medium	The KaxInternalBlock::ReadData function in libMatroska before 1.4.4 allows context-dependent attackers to obtain sensitive information from process heap memory via crafted EBML lacing, which triggers an invalid memory access.	libmatroska	Unchanged	8.0.0.4	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-263
6026	CVE-2015-8791	Medium	Medium	The EbmlElement::ReadCodedSizeValue function in libEBML before 1.3.3 allows context-dependent attackers to obtain sensitive information from process heap memory via a crafted length value in an EBML id, which triggers an invalid memory access.	libebml	Unchanged	8.0.0.3	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-252
6027	CVE-2015-8790	Medium	Medium	The EbmlUnicodeString::UpdateFromUTF8 function in libEBML before 1.3.3 allows context-dependent attackers to obtain sensitive information from process heap memory via a crafted UTF-8 string, which triggers an invalid memory access.	libebml	Unchanged	8.0.0.3	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-262
6028	CVE-2015-8789	High	Critical	Use-after-free vulnerability in the EbmlMaster::Read function in libEBML before 1.3.3 allows context-dependent attackers to have unspecified impact via a deeply nested element with infinite size followed by another element of an upper level in an EBML document.CWE-416: Use After Free	libebml	Unchanged	8.0.0.3	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-232
6029	CVE-2015-8787	HIGH	Critical	The nf_nat_redirect_ipv4 function in net/netfilter/nf_nat_redirect.c in the Linux kernel before 4.4 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by sending certain IPv4 packets to an incompletely configured interface, a related issue to CVE-2003-1604.	linux	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-241
6030	CVE-2015-8785	MEDIUM	Medium	The fuse_fill_write_pages function in fs/fuse/file.c in the Linux kernel before 4.4 allows local users to cause a denial of service (infinite loop) via a writev system call that triggers a zero length for the first segment of an iov.	linux	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-253

	A	B	C	D	E	F	G	H	I	J	K	L	M
6031	CVE-2015-8784	MEDIUM	Medium	A flaw was discovered in a way libtiff decodes special data. A potential out-of-bounds write could occur for specifically crafted images.	tiff	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-277
6032	CVE-2015-8783	MEDIUM	Medium	tif_luv.c in libtiff allows attackers to cause a denial of service (out-of-bounds reads) via a crafted TIFF image.	libtiff	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-260
6033	CVE-2015-8782	MEDIUM	Medium	tif_luv.c in libtiff allows attackers to cause a denial of service (out-of-bounds writes) via a crafted TIFF image, a different vulnerability than CVE-2015-8781.	libtiff	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-256
6034	CVE-2015-8781	MEDIUM	Medium	tif_luv.c in libtiff allows attackers to cause a denial of service (out-of-bounds write) via an invalid number of samples per pixel in a LogL compressed TIFF image, a different vulnerability than CVE-2015-8782.	libtiff	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-242
6035	CVE-2015-8779	HIGH	Critical	A stack overflow vulnerability in the catopen function was found, causing applications which pass long strings to the catopen function to crash or, potentially execute arbitrary code.	glibc	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-245
6036	CVE-2015-8778	High	Critical	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, which triggers out-of-bounds heap-memory access.	glibc	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-472
6037	CVE-2015-8777	Low	Medium	The process_envvars function in elf/rtld.c in the GNU C Library (aka glibc or libc6) before 2.23 allows local users to bypass a pointer-guarding protection mechanism via a zero value of the LD_POINTER_GUARD environment variable.	glibc	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-189
6038	CVE-2015-8776	MEDIUM	Critical	Out-of-range time values passed to the strftime function may cause it to crash, leading to a denial of service, or potentially disclosure information.	glibc	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-222
6039	CVE-2015-8767	MEDIUM	High	net/sctp/sm_sideeffect.c in the Linux kernel before 4.3 does not properly manage the relationship between a lock and a socket, which allows local users to cause a denial of service (deadlock) via a crafted sctp_accept call.	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-236
6040	CVE-2015-8764	MEDIUM	High	Off-by-one error in the EAP-PWD module in FreeRADIUS 3.0 through 3.0.8, which triggers a buffer overflow.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3675
6041	CVE-2015-8763	MEDIUM	High	The EAP-PWD module in FreeRADIUS 3.0 through 3.0.8 allows remote attackers to have unspecified impact via a crafted (1) commit or (2) confirm message, which triggers an out-of-bounds read.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4056
6042	CVE-2015-8762	MEDIUM	Medium	The EAP-PWD module in FreeRADIUS 3.0 through 3.0.8 allows remote attackers to cause a denial of service (NULL pointer dereference and server crash) via a zero-length EAP-PWD packet.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3659
6043	CVE-2015-8746	Medium	High	fs/nfs/nfs4proc.c in the NFS client in the Linux kernel before 4.2.2 does not properly initialize memory for migration recovery operations, which allows remote NFS servers to cause a denial of service (NULL pointer dereference and panic) via crafted network traffic.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-561
6044	CVE-2015-8745	Low	Medium	QEMU (aka Quick Emulator) built with a VMWARE VMXNET3 paravirtual NIC emulator support is vulnerable to crash issue. It could occur while reading Interrupt Mask Registers (IMR). A privileged (CAP_SYS_RAWIO) guest user could use this flaw to crash the QEMU process instance resulting in DoS.	qemu	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3005
6045	CVE-2015-8744	Low	Medium	QEMU (aka Quick Emulator) built with a VMWARE VMXNET3 paravirtual NIC emulator support is vulnerable to crash issue. It occurs when a guest sends a Layer-2 packet smaller than 22 bytes. A privileged (CAP_SYS_RAWIO) guest user could use this flaw to crash the QEMU process instance resulting in DoS.	qemu	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2989
6046	CVE-2015-8743	Low	High	QEMU (aka Quick Emulator) built with the NE2000 device emulation support is vulnerable to an OOB r/w access issue. It could occur while performing 'ioport' r/w operations. A privileged (CAP_SYS_RAWIO) user/process could use this flaw to leak or corrupt QEMU memory bytes.	qemu	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2969
6047	CVE-2015-8742	Medium	Medium	The dissect_CPMSetBindings function in epan/dissectors/packet-mswsp.c in the MS-WSP dissector in Wireshark 2.0.x before 2.0.1 does not validate the column size, which allows remote attackers to cause a denial of service (memory consumption or application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-113
6048	CVE-2015-8741	Medium	Medium	The dissect_ppi function in epan/dissectors/packet-ppi.c in the PPI dissector in Wireshark 2.0.x before 2.0.1 does not initialize a packet-header data structure, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-120
6049	CVE-2015-8740	Medium	Medium	The dissect_tds7_colmetadata_token function in epan/dissectors/packet-tds.c in the TDS dissector in Wireshark 2.0.x before 2.0.1 does not validate the number of columns, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-114
6050	CVE-2015-8739	Medium	Medium	The ipmi_fmt_udpport function in epan/dissectors/packet-ipmi.c in the IPMI dissector in Wireshark 2.0.x before 2.0.1 improperly attempts to access a packet scope, which allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-132
6051	CVE-2015-8738	Medium	Medium	The s7comm_decode_ud_cpu_szl_subfunc function in epan/dissectors/packet-s7comm_szl_ids.c in the S7COMM dissector in Wireshark 2.0.x before 2.0.1 does not validate the list count in an SZL response, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-122

	A	B	C	D	E	F	G	H	I	J	K	L	M
6052	CVE-2015-8737	Medium	Medium	The mp2t_open function in wiretap/mp2t.c in the MP2T file parser in Wireshark 2.0.x before 2.0.1 does not validate the bit rate, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted file.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-139
6053	CVE-2015-8736	Medium	Medium	The mp2t_find_next_pcr function in wiretap/mp2t.c in the MP2T file parser in Wireshark 2.0.x before 2.0.1 does not reserve memory for a trailer, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted file.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-135
6054	CVE-2015-8735	Medium	Medium	The get_value function in epan/dissectors/packet-btatt.c in the Bluetooth Attribute (aka BT ATT) dissector in Wireshark 2.0.x before 2.0.1 uses an incorrect integer data type, which allows remote attackers to cause a denial of service (invalid write operation and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-117
6055	CVE-2015-8734	Medium	Medium	The dissect_nwp function in epan/dissectors/packet-nwp.c in the NWP dissector in Wireshark 2.0.x before 2.0.1 mishandles the packet type, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-105
6056	CVE-2015-8733	Medium	Medium	The ngsniffer_process_record function in wiretap/ngsniffer.c in the Sniffer file parser in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the relationships between record lengths and record header lengths, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted file.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-98
6057	CVE-2015-8732	Medium	Medium	The dissect_zcl_pwr_prof_pwrprofstatersp function in epan/dissectors/packet-zbee-zcl-general.c in the ZigBee ZCL dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the Total Profile Number field, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-118
6058	CVE-2015-8731	Medium	Medium	The dissct_rsl_ipaccess_msg function in epan/dissectors/packet-rsl.c in the RSL dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not reject unknown TLV types, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-109
6059	CVE-2015-8730	Medium	Medium	epan/dissectors/packet-nbap.c in the NBAP dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the number of items, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-127
6060	CVE-2015-8729	Medium	Medium	The ascend_seek function in wiretap/ascendtext.c in the Ascend file parser in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not ensure the presence of a '\0' character at the end of a date string, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted file.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-101
6061	CVE-2015-8728	Medium	Medium	The Mobile Identity parser in (1) epan/dissectors/packet-ansi_a.c in the ANSI A dissector and (2) epan/dissectors/packet-gsm_a_common.c in the GSM A dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 improperly uses the tvb_bcd_dig_to_wmem_packet_str function, which allows remote attackers to cause a denial of service (buffer overflow and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-99
6062	CVE-2015-8727	Medium	Medium	The dissect_rsvp_common function in epan/dissectors/packet-rsvp.c in the RSVP dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not properly maintain request-key data, which allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-131
6063	CVE-2015-8726	Medium	Medium	wiretap/vwr.c in the VeriWave file parser in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate certain signature and Modulation and Coding Scheme (MCS) data, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted file.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-125
6064	CVE-2015-8725	Medium	Medium	The dissect_diameter_base_framed_ipv6_prefix function in epan/dissectors/packet-diameter.c in the DIAMETER dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the IPv6 prefix length, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-134
6065	CVE-2015-8724	Medium	Medium	The AirPDcapDecryptWPABroadcastKey function in epan/crypt/airpdcap.c in the 802.11 dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not verify the WPA broadcast key length, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-129
6066	CVE-2015-8723	Medium	Medium	The AirPDcapPacketProcess function in epan/crypt/airpdcap.c in the 802.11 dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the relationship between the total length and the capture length, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-121
6067	CVE-2015-8722	Medium	Medium	epan/dissectors/packet-sctp.c in the SCTP dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate the frame pointer, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-115

	A	B	C	D	E	F	G	H	I	J	K	L	M
6068	CVE-2015-8721	Medium	Medium	Buffer overflow in the tvb_uncompress function in epan/tvbuff_zlib.c in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 allows remote attackers to cause a denial of service (application crash) via a crafted packet with zlib compression.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-112
6069	CVE-2015-8720	Medium	Medium	The dissect_ber_GeneralizedTime function in epan/dissectors/packet-ber.c in the BER dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 improperly checks an sscanf return value, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-106
6070	CVE-2015-8719	Medium	Medium	The dissect_dns_answer function in epan/dissectors/packet-dns.c in the DNS dissector in Wireshark 1.12.x before 1.12.9 mishandles the EDNS0 Client Subnet option, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-133
6071	CVE-2015-8718	Medium	Medium	Double free vulnerability in epan/dissectors/packet-nlm.c in the NLM dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1, when the Match MSG/RES packets for async NLM option is enabled, allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-140
6072	CVE-2015-8717	Medium	Medium	The dissect_sdp function in epan/dissectors/packet-sdp.c in the SDP dissector in Wireshark 1.12.x before 1.12.9 does not prevent use of a negative media count, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-96
6073	CVE-2015-8716	Medium	Medium	The init_t38_info_conv function in epan/dissectors/packet-t38.c in the T.38 dissector in Wireshark 1.12.x before 1.12.9 does not ensure that a conversation exists, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-107
6074	CVE-2015-8715	Medium	Medium	epan/dissectors/packet-alljoyn.c in the AllJoyn dissector in Wireshark 1.12.x before 1.12.9 does not check for empty arguments, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-138
6075	CVE-2015-8714	Medium	Medium	The dissect_dcom_OBJREF function in epan/dissectors/packet-dcom.c in the DCOM dissector in Wireshark 1.12.x before 1.12.9 does not initialize a certain IPv4 data structure, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-94
6076	CVE-2015-8713	Medium	Medium	epan/dissectors/packet-umts_fp.c in the UMTS FP dissector in Wireshark 1.12.x before 1.12.9 does not properly reserve memory for channel ID mappings, which allows remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-104
6077	CVE-2015-8712	Medium	Medium	The dissect_hsdsch_channel_info function in epan/dissectors/packet-umts_fp.c in the UMTS FP dissector in Wireshark 1.12.x before 1.12.9 does not validate the number of PDUs, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-111
6078	CVE-2015-8711	Medium	Medium	epan/dissectors/packet-nbap.c in the NBAP dissector in Wireshark 1.12.x before 1.12.9 and 2.0.x before 2.0.1 does not validate conversation data, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-100
6079	CVE-2015-8710	HIGH	Critical	It was discovered that libxml2 could access out-of-bounds memory when parsing unclosed HTML comments. A remote attacker could provide a specially crafted XML file that, when processed by an application linked against libxml2, could cause the application to disclose heap memory contents.	libxml2	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-283
6080	CVE-2015-8709	MEDIUM	High	Linux kernel built with the User Namespaces(CONFIG_USER_NS) support is vulnerable to a potential privilege escalation flaw. It could occur when a root owned process tries to enter a user namespace, wherein a user attempts to attach the entering process via ptrace(1). A privileged name space user could use this flaw to potentially escalate their privileges on the system.	linux	Unchanged	8.0.0.22	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-108
6081	CVE-2015-8705	Medium	High	buffer.c in named in ISC BIND 9.10.x before 9.10.3-P3, when debug logging is enabled, allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit, or daemon crash) or possibly have unspecified other impact via (1) OPT data or (2) an ECS option.	bind	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-151
6082	CVE-2015-8704	Medium	Medium	apl_42.c in ISC BIND 9.x before 9.9.8-P3 and 9.9.x and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record.	bind	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-150
6083	CVE-2015-8701	Low	Medium	QEMU (aka Quick Emulator) built with the Rocker switch emulation support is vulnerable to an off-by-one error. It happens while processing transmit (tx) descriptors in 'tx_consume' routine, if a descriptor has to have more than allowed (ROCKER_TX_FRAGS_MAX=16) fragments. A privileged user inside guest could use this flaw to cause memory leakage on the host or crash the QEMU process instance resulting in DoS issue.	qemu	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2956
6084	CVE-2015-8683	MEDIUM	Medium	An out-bounds-read flaw was found in the way libtiff processed CIE Lab image format files. A attacker could create a specially-crafted CIE Lab image format files which could cause libtiff to crash.	tiff	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-270
6085	CVE-2015-8669	Medium	Medium	libraries/config/messages.inc.php in phpMyAdmin 4.0.x before 4.0.10.12, 4.4.x before 4.4.15.2, and 4.5.x before 4.5.3.1 allows remote attackers to obtain sensitive information via a crafted request, which reveals the full path in an error message.	phpmyadmin	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-72

	A	B	C	D	E	F	G	H	I	J	K	L	M
6086	CVE-2015-8668	HIGH	Critical	Heap-based buffer overflow in the PackBitsPreEncode function in tif_packbits.c in bmp2tiff in libtiff 4.0.6 and earlier allows remote attackers to execute arbitrary code or cause a denial of service via a large width field in a BMP image.	libtiff	Unchanged	Investigate	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-126
6087	CVE-2015-8666	Low	Medium	Heap-based buffer overflow in QEMU, when built with the Q35-chipset-based PC system emulator.	qemu	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4030
6088	CVE-2015-8665	MEDIUM	Medium	An Out-of-bounds read flaw was found in libtiff. An attacker could create a specially-crafted TIFF file, which could cause libtiff to crash.	tiff	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-269
6089	CVE-2015-8663	High	High	The ff_get_buffer function in libavcodec/utils.c in FFmpeg before 2.8.4 preserves width and height values after a failure, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via a crafted .mov file.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-57
6090	CVE-2015-8662	High	High	The ff_dwt_decode function in libavcodec/jpeg2000dwt.c in FFmpeg before 2.8.4 does not validate the number of decomposition levels before proceeding with Discrete Wavelet Transform decoding, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG 2000 data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-74
6091	CVE-2015-8661	High	High	The h264_slice_header_init function in libavcodec/h264_slice.c in FFmpeg before 2.8.3 does not validate the relationship between the number of threads and the number of slices, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted H.264 data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-76
6092	CVE-2015-8660	High	Medium	The ovl_setattr function in fs/overlayfs/inode.c in the Linux kernel through 4.3.3 attempts to merge distinct setattr operations, which allows local users to bypass intended access restrictions and modify the attributes of arbitrary overlay files via a crafted application.	linux	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-77
6093	CVE-2015-8631	MEDIUM	Medium	Multiple memory leaks in kadmin/server/server_stubs.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13.4 and 1.14.x before 1.14.1 allow remote authenticated users to cause a denial of service (memory consumption) via a request specifying a NULL principal name.	krb5	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-257
6094	CVE-2015-8630	MEDIUM	High	The (1) kadm5_create_principal_3 and (2) kadm5_modify_principal functions in lib/kadm5/srv/svr_principal.c in kadmind in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.4 and 1.14.x before 1.14.1 allow remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) by specifying KADM5_POLICY with a NULL policy name.	krb5	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-247
6095	CVE-2015-8629	LOW	Low	The xdr_nullstring function in lib/kadm5/kadm_rpc_xdr.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13.4 and 1.14.x before 1.14.1 does not verify whether \0' characters exist as expected, which allows remote authenticated users to obtain sensitive information or cause a denial of service (out-of-bounds read) via a crafted string.	krb5	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-226
6096	CVE-2015-8617	High	Critical	Format string vulnerability in the zend_throw_or_error function in Zend/zend_execute_API.c in PHP 7.x before 7.0.1 allows remote attackers to execute arbitrary code via format string specifiers in a string that is misused as a class name, leading to incorrect error handling.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-161
6097	CVE-2015-8616	High	High	Use-after-free vulnerability in the Collator::sortWithSortKeys function in ext/intl/collator/collator_sort.c in PHP 7.x before 7.0.1 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging the relationships between a key buffer and a destroyed array.CWE-416: Use After Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-167
6098	CVE-2015-8613	Low	Medium	Stack-based buffer overflow in the megasas_ctrl_get_info function in QEMU, when built with SCSI MegaRAID SAS HBA emulation support, allows local guest users to cause a denial of service (QEMU instance crash) via a crafted SCSI controller CTRL_GET_INFO command.	qemu	Unchanged	8.0.0.18	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4013
6099	CVE-2015-8608	HIGH	Critical	avoid invalid memory access in MapPath[AW]	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1269
6100	CVE-2015-8607	High	High	The canonpath function in the File::Spec module in PathTools before 3.62, as used in Perl, does not properly preserve the taint attribute of data, which might allow context-dependent attackers to bypass the taint protection mechanism via a crafted string.	perl	Unchanged	8.0.0.9	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1296
6101	CVE-2015-8605	Medium	Medium	ISC DHCP 4.x before 4.1-ESV-R12-P1 and 4.2.x and 4.3.x before 4.3.3-P1 allows remote attackers to cause a denial of service (application crash) via an invalid length field in a UDP IPv4 packet.	dhcp	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-187
6102	CVE-2015-8575	LOW	Medium	The sco_sock_bind function in net/bluetooth/sco.c in the Linux kernel before 4.3.4 does not verify an address length, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism via a crafted application.	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-258
6103	CVE-2015-8569	Low	Low	The (1) pptp_bind and (2) pptp_connect functions in drivers/net/ppp/pptp.c in the Linux kernel through 4.3.3 do not verify an address length, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism via a crafted application.	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-60
6104	CVE-2015-8568	Medium	Medium	Memory leak in QEMU, when built with a VMWARE VMXNET3 paravirtual NIC emulator support, allows local guest users to cause a denial of service (host memory consumption) by trying to activate the vmxnet3 device repeatedly.	qemu	Unchanged	8.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4098

	A	B	C	D	E	F	G	H	I	J	K	L	M
6105	CVE-2015-8567	Medium	High	Memory leak in net/vmxnet3.c in QEMU allows remote attackers to cause a denial of service (memory consumption).	qemu	Unchanged	8.0.0.18	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4077
6106	CVE-2015-8560	HIGH	High	It was discovered that foomatic-rip failed to remove all shell special characters from inputs used to construct command lines for external programs run by the filter. An attacker could possibly use this flaw to execute arbitrary commands.	foomatic-filters	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-287
6107	CVE-2015-8558	Medium	Medium	The ehci_process_itd function in hw/usb/hcd-ehci.c in QEMU allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) via a circular isochronous transfer descriptor (iTD) list.	qemu	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-742
6108	CVE-2015-8543	Medium	High	The networking implementation in the Linux kernel through 4.3.3, as used in Android and other products, does not validate protocol identifiers for certain protocol families, which allows local users to cause a denial of service (NULL function pointer dereference and system crash) or possibly gain privileges by leveraging CLONE_NEWUSER support to execute a crafted SOCK_RAW application.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-67
6109	CVE-2015-8540	High	High	Integer underflow in the png_check_keyword function in pngwutil.c in libpng 0.90 through 0.99, 1.0.x before 1.0.66, 1.1.x and 1.2.x before 1.2.56, 1.3.x and 1.4.x before 1.4.19, and 1.5.x before 1.5.26 allows remote attackers to have unspecified impact via a space character as a keyword in a PNG image, which triggers an out-of-bounds read.	libpng	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-489
6110	CVE-2015-8539	HIGH	High	The KEYS subsystem in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (BUG) via crafted keyctl commands that negatively instantiate a key, related to security/keys/encrypted-keys/encrypted.c, security/keys/trusted.c, and security/keys/user_defined.c.	linux	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-233
6111	CVE-2015-8504	LOW	Medium	An arithmetic-exception flaw was found in the QEMU emulator built with VNC display-driver support. The VNC server incorrectly handled 'SetPixelFormat' messages sent from clients. A privileged remote client could use this flaw to crash the guest resulting in denial of service.	qemu	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-278
6112	CVE-2015-8472	High	High	Buffer overflow in the png_set_PLTE function in libpng before 1.0.65, 1.1.x and 1.2.x before 1.2.55, 1.3.x, 1.4.x before 1.4.18, 1.5.x before 1.5.25, and 1.6.x before 1.6.20 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8126.	libpng	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-177
6113	CVE-2015-8470			The console in Puppet Enterprise 3.7.x, 3.8.x, and 2015.2.x does not set the secure flag for the JSESSIONID cookie in an HTTPS session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an HTTP session.	puppet	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2765
6114	CVE-2015-8467	Medium	High	The samldb_check_user_account_control_acl function in dsdb/samdb/ldb_modules/samldb.c in Samba 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3 does not properly check for administrative privileges during creation of machine accounts, which allows remote authenticated users to bypass intended access restrictions by leveraging the existence of a domain with both a Samba DC and a Windows DC, a similar issue to CVE-2015-2535.	samba	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-124
6115	CVE-2015-8461	High		Race condition in resolver.c in named in ISC BIND 9.9.8 before 9.9.8-P2 and 9.10.3 before 9.10.3-P2 allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via unspecified vectors.	bind	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-71
6116	CVE-2015-8395	High		PCRE before 8.38 mishandles certain references, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, a related issue to CVE-2015-8384 and CVE-2015-8392.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2224
6117	CVE-2015-8394	High		PCRE before 8.38 mishandles the (?(<digits>) and (?(R<digits>) conditions, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2209
6118	CVE-2015-8393	Medium		pcregrep in PCRE before 8.38 mishandles the -q option for binary files, which might allow remote attackers to obtain sensitive information via a crafted file, as demonstrated by a CGI script that sends stdout data to a client.	pcre	Unchanged	8.0.0.1	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2197
6119	CVE-2015-8392	High		PCRE before 8.38 mishandles certain instances of the (?| substring, which allows remote attackers to cause a denial of service (unintended recursion and buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, a related issue to CVE-2015-8384 and CVE-2015-8395.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2213
6120	CVE-2015-8391	High		The pcre_compile function in pcre_compile.c in PCRE before 8.38 mishandles certain [; nesting, which allows remote attackers to cause a denial of service (CPU consumption) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2204

	A	B	C	D	E	F	G	H	I	J	K	L	M
6121	CVE-2015-8390	High		PCRE before 8.38 mishandles the [: and \\ substrings in character classes, which allows remote attackers to cause a denial of service (uninitialized memory read) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2194
6122	CVE-2015-8389	High		PCRE before 8.38 mishandles the /(?:|a|){100}x/ pattern and related patterns, which allows remote attackers to cause a denial of service (infinite recursion) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2199
6123	CVE-2015-8388	High		PCRE before 8.38 mishandles the /(?=di(?<=(?1)))((?=(.)))/ pattern and related patterns with an unmatched closing parenthesis, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2193
6124	CVE-2015-8387	High		PCRE before 8.38 mishandles (?123) subroutine calls and related subroutine calls, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2218
6125	CVE-2015-8386	High		PCRE before 8.38 mishandles the interaction of lookbehind assertions and mutually recursive subpatterns, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2215
6126	CVE-2015-8385	High		PCRE before 8.38 mishandles the /(?|(\k'Pm')|(?'Pm'))/ pattern and related patterns with certain forward references, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2211
6127	CVE-2015-8384	High		PCRE before 8.38 mishandles the /(?J)(?'d'(?'d\g{d}))/ pattern and related patterns with certain recursive back references, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, a related issue to CVE-2015-8392 and CVE-2015-8395.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2222
6128	CVE-2015-8383	High		PCRE before 8.38 mishandles certain repeated conditional groups, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2202
6129	CVE-2015-8382	Medium		The match function in pcre_exec.c in PCRE before 8.37 mishandles the /(?:((abcd))|(((?:(?:(?:(?:abc|(?:abcdef)))|b)abcdefghi)abc)|((*ACCEPT)))/ pattern and related patterns involving (*ACCEPT), which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (partially initialized memory and application crash) via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror, aka ZDI-CAN-2547.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2212
6130	CVE-2015-8381	High		The compile_regex function in pcre_compile.c in PCRE before 8.38 and pcre2_compile.c in PCRE2 before 10.2x mishandles the /(?J:(?|(:(?)(?'R')(\k'R')|((?'R'))H'Rk'Rf)|s(?'R'))))/ and /(?J:(?|(:(?|(?'R')(\z(?)(?'R')(\k'R'))|((?'R'))k'R')|((?'R'))H'AkRf)|s(?'R')))/ patterns, and related patterns with certain group references, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2195
6131	CVE-2015-8380	High		The pcre_exec function in pcre_exec.c in PCRE before 8.38 mishandles a // pattern with a \01 string, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2216
6132	CVE-2015-8374	Low	Medium	fs/btrfs/inode.c in the Linux kernel before 4.3.3 mishandles compressed inline extents, which allows local users to obtain sensitive pre-truncation information from a file via a clone action.	linux	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-70
6133	CVE-2015-8370	Medium		Multiple integer underflows in Grub2 1.98 through 2.02 allow physically proximate attackers to bypass authentication, obtain sensitive information, or cause a denial of service (disk corruption) via backspace characters in the (1) grub_username_get function in grub-core/normal/auth.c or the (2) grub_password_get function in lib/crypto.c, which trigger an Off-by-two or Out of bounds overwrite memory error.	grub2	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-62
6134	CVE-2015-8365	MEDIUM		The smka_decode_frame function in libavcodec/smacker.c in FFmpeg before 2.6.5, 2.7.x before 2.7.3, and 2.8.x through 2.8.2 does not verify that the data size is consistent with the number of channels, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Smacker data.	gst-ffmpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1920

	A	B	C	D	E	F	G	H	I	J	K	L	M
6135	CVE-2015-8364	MEDIUM		Integer overflow in the ff_ivi_init_planes function in libavcodec/ivi.c in FFmpeg before 2.6.5, 2.7.x before 2.7.3, and 2.8.x through 2.8.2 allows remote attackers to cause a denial of service (out-of-bounds heap-memory access) or possibly have unspecified other impact via crafted image dimensions in Indeo Video Interactive data.	gst-ffmpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1925
6136	CVE-2015-8363	MEDIUM		The jpeg2000_read_main_headers function in libavcodec/jpeg2000dec.c in FFmpeg before 2.6.5, 2.7.x before 2.7.3, and 2.8.x through 2.8.2 does not enforce uniqueness of the SIZ marker in a JPEG 2000 image, which allows remote attackers to cause a denial of service (out-of-bounds heap-memory access) or possibly have unspecified other impact via a crafted image with two or more of these markers.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1906
6137	CVE-2015-8345	LOW	Medium	An infinite-loop flaw was discovered in the QEMU emulator built with i8255x (PRO100) emulation support. When processing a chain of commands located in the Command Block List(CBL), each Command Block(CB) points to the next command in the list. If the link to the next CB pointed to the same block or if there was a closed loop in the chain, an infinite loop would execute the same command over and over again. A privileged user inside the guest could use this flaw to crash the QEMU instance, resulting in denial of service.	qemu	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-281
6138	CVE-2015-8327	High		Incomplete blacklist vulnerability in util.c in foomatic-rip in cups-filters 1.0.42 before 1.2.0 and in foomatic-filters in Foomatic 4.0.x allows remote attackers to execute arbitrary commands via ` (backtick) characters in a print job.CWE-184: Incomplete Blacklist	foomatic-filters	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-288
6139	CVE-2015-8325	High	High	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.	openssh	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-629
6140	CVE-2015-8324	Medium	Medium	The ext4 implementation in the Linux kernel before 2.6.34 does not properly track the initialization of certain data structures, which allows physically proximate attackers to cause a denial of service (NULL pointer dereference and panic) via a crafted USB device, related to the ext4_fill_super function.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-608
6141	CVE-2015-8317	Medium		The xmlParseXMLDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive information via an (1) unterminated encoding value or (2) incomplete XML declaration in XML data, which triggers an out-of-bounds heap read.	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-78
6142	CVE-2015-8308	MEDIUM	High	LXDM before 0.5.2 did not start X server with -auth, which allows local users to bypass authentication with X connections.	lxdm	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5128
6143	CVE-2015-8242	MEDIUM		libxml2: Stack-based buffer overread vulnerability with HTML parser in push mode in xmlSAX2TextNode causing segmentation fault when compiled with ASAN.	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2200
6144	CVE-2015-8241	Medium		The xmlNextChar function in libxml2 2.9.2 does not properly check the state, which allows context-dependent attackers to cause a denial of service (heap-based buffer over-read and application crash) or obtain sensitive information via crafted XML data.	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-75
6145	CVE-2015-8239	MEDIUM	High	The SHA-2 digest support in the sudoers plugin in sudo after 1.8.7 allows local users with write permissions to parts of the called command to replace them before it is executed.	sudo	Unchanged	8.0.0.24	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5577
6146	CVE-2015-8219	High		The init_tile function in libavcodec/jpeg2000dec.c in FFmpeg before 2.8.2 does not enforce minimum-value and maximum-value constraints on tile coordinates, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG 2000 data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1921
6147	CVE-2015-8218	Medium		The decode_uncompressed function in libavcodec/faxcompr.c in FFmpeg before 2.8.2 does not validate uncompressed runs, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted CCITT FAX data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1907
6148	CVE-2015-8217	High		The ff_hevc_parse_sps function in libavcodec/hevc_ps.c in FFmpeg before 2.8.2 does not validate the Chroma Format Indicator, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted High Efficiency Video Coding (HEVC) data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1913
6149	CVE-2015-8216	High		The ljpeg_decode_yuv_scan function in libavcodec/mjpegdec.c in FFmpeg before 2.8.2 omits certain width and height checks, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted MJPEG data.	gst-ffmpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1902
6150	CVE-2015-8215	Medium		net/ipv6/addrconf.c in the IPv6 stack in the Linux kernel before 4.0 does not validate attempted changes to the MTU value, which allows context-dependent attackers to cause a denial of service (packet loss) via a value that is (1) smaller than the minimum compliant value or (2) larger than the MTU of an interface, as demonstrated by a Router Advertisement (RA) message that is not validated by a daemon, a different vulnerability than CVE-2015-0272. NOTE: the scope of CVE-2015-0272 is limited to the NetworkManager product.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1930

	A	B	C	D	E	F	G	H	I	J	K	L	M
6151	CVE-2015-8214	High		Siemens SIMATIC CP 343-1 Advanced devices before 3.0.44, CP 343-1 Lean devices, CP 343-1 devices, TIM 3V-IE devices, TIM 3V-IE Advanced devices, TIM 3V-IE DNP3 devices, TIM 4R-IE devices, TIM 4R-IE DNP3 devices, CP 443-1 devices, and CP 443-1 Advanced devices might allow remote attackers to obtain administrative access via a session on TCP port 102.	WRLinux doesn't ship SIMATIC	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2220
6152	CVE-2015-8158	MEDIUM	Medium	A flaw was found in the way the ntpq client certain processed incoming packets in a loop in the getresponse() function:	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-165
6153	CVE-2015-8140	MEDIUM	Medium	The ntpq protocol is vulnerable to replay attacks. The sequence number being included under the signature fails to prevent replay attacks for two reasons. Commands that don't require authentication can be used to move the sequence number forward, and NTP doesn't actually care what sequence number is used so a packet can be replayed at any time. If, for example, an attacker can intercept authenticated reconfiguration commands that would. for example, tell ntpd to connect with a server that turns out to be malicious and a subsequent reconfiguration directive removed that malicious server, the attacker could replay the configuration command to re-establish an association to malicious server.	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-207
6154	CVE-2015-8139	MEDIUM	Medium	To prevent off-path attackers from impersonating legitimate peers, clients require that the origin timestamp in a received response packet match the transmit timestamp from its last request to a given peer. Under assumption that only the recipient of the request packet will know the value of the transmit timestamp, this prevents an attacker from forging replies	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-202
6155	CVE-2015-8138	MEDIUM	Medium	The TEST2 check of the originate timestamp in received packets, which requires the timestamp to match the value of the peer->aorg variable and which is supposed to be random to prevent spoofing attacks has been found to be faulty.	ntp	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-192
6156	CVE-2015-8126	High		Multiple buffer overflows in the (1) png_set_PLTE and (2) png_get_PLTE functions in libpng before 1.0.64, 1.1.x and 1.2.x before 1.2.54, 1.3.x and 1.4.x before 1.4.17, 1.5.x before 1.5.24, and 1.6.x before 1.6.19 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image.	libpng	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1919
6157	CVE-2015-8104	Medium		The KVM subsystem in the Linux kernel through 4.2.6, and Xen 4.3.x through 4.6.x, allows guest OS users to cause a denial of service (host OS panic or hang) by triggering many #DB (aka Debug) exceptions, related to svm.c.	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1931
6158	CVE-2015-8100	Low		The net-snmp package in OpenBSD through 5.8 uses 0644 permissions for snmpd.conf, which allows local users to obtain sensitive community information by reading this file.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1576
6159	CVE-2015-8080	Medium	High	Integer overflow in the getnum function in lua_struct.c in Redis 2.8.x before 2.8.24 and 3.0.x before 3.0.6 allows context-dependent attackers with permission to run Lua code in a Redis session to cause a denial of service (memory corruption and application crash) or possibly bypass intended sandbox restrictions via a large number, which triggers a stack-based buffer overflow.	redis	Unchanged	8.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-476
6160	CVE-2015-8041	Medium		Multiple integer overflows in the NDEF record parser in hostapd before 2.5 and wpa_supplicant before 2.5 allow remote attackers to cause a denial of service (process crash or infinite loop) via a large payload length field value in an (1) WPS or (2) P2P NFC NDEF record, which triggers an out-of-bounds read.	hostapd & wpa_supplicant.	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1580
6161	CVE-2015-8036	Medium		Heap-based buffer overflow in ARM mbed TLS (formerly PolarSSL) 1.3.x before 1.3.14 and 2.x before 2.1.2 allows remote SSL servers to cause a denial of service (client crash) and possibly execute arbitrary code via a long session ticket name to the session ticket extension, which is not properly handled when creating a ClientHello message to resume a session. NOTE: this identifier was SPLIT from CVE-2015-5291 per ADT3 due to different affected version ranges.	polarssl	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1570
6162	CVE-2015-8035	Low		The xz_decomp function in xzlib.c in libxml2 2.9.1 does not properly detect compression errors, which allows context-dependent attackers to cause a denial of service (process hang) via crafted XML data.	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1928
6163	CVE-2015-8026	MEDIUM	High	Heap-based buffer overflow in the verify_vbr_checksum function in exfatfsck in exfat-utils before 1.2.1 allows remote attackers to cause a denial of service (infinite loop) or possibly execute arbitrary code via a crafted filesystem.	exfat-utils	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3779
6164	CVE-2015-8023	Medium		The server implementation of the EAP-MSCHAPv2 protocol in the eap-mschapv2 plugin in strongSwan 4.2.12 through 5.x before 5.3.4 does not properly validate local state, which allows remote attackers to bypass authentication via an empty Success message in response to an initial Challenge message.	strongswan	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1903
6165	CVE-2015-8019	High	High	The skb_copy_and_csum_datagram_iovec function in net/core/datagram.c in the Linux kernel 3.14.54 and 3.18.22 does not accept a length argument, which allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact via a write system call followed by a recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-591
6166	CVE-2015-8012	MEDIUM	HIGH	lldpd before 0.8.0 allows remote attackers to cause a denial of service (assertion failure and daemon crash) via a malformed packet.	lldpd	Unchanged	8.0.0.33	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3987

	A	B	C	D	E	F	G	H	I	J	K	L	M
6167	CVE-2015-8011	MEDIUM	CRITICAL	Buffer overflow in the lldp_decode function in daemon/protocols/lldp.c in lldpd before 0.8.0 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via vectors involving large management addresses and TLV boundaries.	lldpd	Unchanged	8.0.0.33	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3988
6168	CVE-2015-8000	Medium		db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.	bind	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-65
6169	CVE-2015-7995	Medium		The xsltStylePreCompute function in preproc.c in libxslt 1.1.28 does not check if the parent node is an element, which allows attackers to cause a denial of service via a crafted XML file, related to a type confusion issue.CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')	libxslt	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1923
6170	CVE-2015-7990	Medium	Medium	Race condition in the rds_sendmsg function in net/rds/sendmsg.c in the Linux kernel before 4.3.3 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by using a socket that was not properly bound. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-6937.	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-64
6171	CVE-2015-7981	Medium		The png_convert_to_rfc1123 function in png.c in libpng 1.0.x before 1.0.64, 1.2.x before 1.2.54, and 1.4.x before 1.4.17 allows remote attackers to obtain sensitive process memory information via crafted tIME chunk data in an image file, which triggers an out-of-bounds read.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1901
6172	CVE-2015-7979	MEDIUM	High	It was found that when NTP is configured in broadcast mode, an off-path attacker could broadcast packets with bad authentication (wrong key, mismatched key, incorrect MAC, etc) to all clients. The clients, upon receiving the malformed packets, would break the association with the broadcast server. This could cause the time on affected clients to become out of sync over a longer period of time.	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-200
6173	CVE-2015-7978	MEDIUM	High	A stack-based buffer overflow was found in the way ntpd processed 'ntpdc reslist' commands that queried restriction lists with a large amount of entries. A remote attacker could use this flaw to crash the ntpd process.	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-190
6174	CVE-2015-7977	MEDIUM	Medium	A NULL pointer dereference flaw was found in the way ntpd processed 'ntpdc reslist' commands that queried restriction lists with a large amount of entries. A remote attacker could use this flaw to crash the ntpd process.	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-197
6175	CVE-2015-7976	MEDIUM	Medium	The ntpq saveconfig command does not do adequate filtering of special characters from the supplied filename. Note: the ability to use the saveconfig command is controlled by the 'restrict nomodify' directive, and the recommended default configuration is to disable this capability. If the ability to execute a 'saveconfig' is required, it can easily (and should) be limited and restricted to a known small number of IP addresses.	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-179
6176	CVE-2015-7975	LOW	Medium	It was found that ntpq did not implement a proper lenght check when calling nextvar(), which executes a memcpy(), on the name buffer.	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-195
6177	CVE-2015-7974	LOW	Medium	NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when authenticating packets, which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a skeleton key.	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-159
6178	CVE-2015-7973	MEDIUM	Medium	It was found that when NTP is configured in broadcast mode, a man-in-the-middle attacker or a malicious client could replay packets received from the broadcast server to all (other) clients. This could cause the time on affected clients to become out of sync over a longer period of time.	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-181
6179	CVE-2015-7942	Medium		The xmlParseConditionalSections function in parser.c in libxml2 does not properly skip intermediary entities when it stops parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted XML data, a different vulnerability than CVE-2015-7941.	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1929
6180	CVE-2015-7941	Medium		libxml2 2.9.2 does not properly stop parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and libxml2 crash) via crafted XML data to the (1) xmlParseEntityDecl or (2) xmlParseConditionalSections function in parser.c, as demonstrated by non-terminated entities.context dependent seems to point to MiTM attack due to: If a user or automated system were tricked into opening a specially crafted document, an attacker could possibly cause libxml2 to crash, resulting in a denial of service. This issue only affected Ubuntu 12.04 LTS, Ubuntu 14.04 LTS and Ubuntu 15.04.	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1926
6181	CVE-2015-7885	Low	Low	The dgnc_mgmt_ioctl function in drivers/staging/dgnc/dgnc_mgmt.c in the Linux kernel through 4.3.3 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel memory via a crafted application.	linux	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-68
6182	CVE-2015-7884	Low	Low	The vivid_fb_ioctl function in drivers/media/platform/vivid/vivid-osd.c in the Linux kernel through 4.3.3 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel memory via a crafted application.	linux	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-63
6183	CVE-2015-7882	Medium	HIGH	Improper handling of LDAP authentication in MongoDB Server versions 3.0.0 to 3.0.6 allows an unauthenticated client to gain unauthorized access.	mongodb	Unchanged	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-4556
6184	CVE-2015-7873	Medium		The redirection feature in url.php in phpMyAdmin 4.4.x before 4.4.15.1 and 4.5.x before 4.5.1 allows remote attackers to spoof content via the url parameter.	phpmyadmin	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1356

	A	B	C	D	E	F	G	H	I	J	K	L	M
6185	CVE-2015-7872	Low		The key_gc_unused_keys function in security/keys/gc.c in the Linux kernel through 4.2.6 allows local users to cause a denial of service (OOPS) via crafted keyctl commands.	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1905
6186	CVE-2015-7871	HIGH	Critical	Unauthenticated off-path attackers can force ntpd processes to peer with malicious time sources of the attacker??s choosing allowing the attacker to make arbitrary changes to system time. This attack leverages a logic error in ntpd??s handling of certain crypto-NAK packets. When a vulnerable ntpd receives an NTP symmetric active crypto-NAK packet, it will peer with the sender bypassing the authentication typically required to establish a peer association.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1189
6187	CVE-2015-7855	MEDIUM	Medium	It was found that NTP's decodenetnum() would abort with an assertion failure when processing a mode 6 or mode 7 packet containing an unusually long data value where a network address was expected. This could allow an authenticated attacker to crash ntpd.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1231
6188	CVE-2015-7854	MEDIUM	High	A potential buffer overflow vulnerability exists in the password management functionality of ntp. A specially crafted key file could cause a buffer overflow potentially resulting in memory being modified. An attacker could provide a malicious password to trigger this vulnerability.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1190
6189	CVE-2015-7853	HIGH	Critical	A potential buffer overflow vulnerability exists in the refclock of ntpd. An invalid length provided by a hardware reference clock could cause a buffer overflow potentially resulting in memory being modified. A malicious reflock could provide a negative length to trigger this vulnerability.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1192
6190	CVE-2015-7852	MEDIUM	Medium	A potential off by one vulnerability exists in the cookedprint functionality of ntpq. A specially crafted buffer could cause a buffer overflow potentially resulting in null byte being written out of bounds.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1193
6191	CVE-2015-7851			A potential path traversal vulnerability exists in the config file saving of ntpd on VMS. A specially crafted path could cause a path traversal potentially resulting in files being overwritten. An attacker could provide a malicious path to trigger this vulnerability. #####Tested Versions	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1195
6192	CVE-2015-7850	MEDIUM	Medium	An exploitable denial of service vulnerability exists in the remote configuration functionality of the Network Time Protocol. A specially crafted configuration file could cause an endless loop resulting in a denial of service. An attacker could provide a the malicious configuration file to trigger this vulnerability.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1196
6193	CVE-2015-7849	MEDIUM	High	An exploitable use-after-free vulnerability exists in the password management functionality of the Network Time Protocol. A specially crafted key file could cause a buffer overflow resulting in memory corruption. An attacker could provide a malicious password file to trigger this vulnerability.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1197
6194	CVE-2015-7848	MEDIUM	High	When processing a specially crafted private mode packet, an integer overflow can occur leading to out of bounds memory copy operation. The crafted packet needs to have the correct message authentication code and a valid timestamp. When processed by the NTP daemon, it leads to an immediate crash.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1198
6195	CVE-2015-7833	Medium		The usbvision driver in the Linux kernel package 3.10.0-123.20.1.el7 through 3.10.0-229.14.1.el7 in Red Hat Enterprise Linux (RHEL) 7.1 allows physically proximate attackers to cause a denial of service (panic) via a nonzero bInterfaceNumber value in a USB device descriptor.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-221
6196	CVE-2015-7830	Medium		The pcapng_read_if_descr_block function in wiretap/pcapng.c in the pcapng parser in Wireshark 1.12.x before 1.12.8 uses too many levels of pointer indirection, which allows remote attackers to cause a denial of service (incorrect free and application crash) via a crafted packet that triggers interface-filter copying.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1900
6197	CVE-2015-7805	High		Heap-based buffer overflow in libsndfile 1.0.25 allows remote attackers to have unspecified impact via the headindex value in the header in an AIFF file.	libsndfile	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1922
6198	CVE-2015-7804	Medium		Off-by-one error in the phar_parse_zipfile function in ext/phar/zip.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (uninitialized pointer dereference and application crash) by including the / filename in a .zip PHAR archive.	php	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2217
6199	CVE-2015-7803	Medium		The phar_get_entry_data function in ext/phar/util.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a .phar file with a crafted TAR archive entry in which the Link indicator references a file that does not exist.CWE-476: NULL Pointer Dereference	php	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2192
6200	CVE-2015-7799	Medium		The slhc_init function in drivers/net/slip/slhc.c in the Linux kernel through 4.2.3 does not ensure that certain slot numbers are valid, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted PPPIOCSMAXCID ioctl call.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-224
6201	CVE-2015-7744	Low	Medium	wolfSSL (formerly CyaSSL) before 3.6.8 does not properly handle faults associated with the Chinese Remainder Theorm (CRT) process when allowing ephemeral key exchange without low memory optimizations on a server, which makes it easier for remote attackers to obtain private RSA keys by capturing TLS handshakes, aka a Lenstra attack.	wolfssl	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-186

	A	B	C	D	E	F	G	H	I	J	K	L	M
6202	CVE-2015-7705	HIGH	Critical	A flaw was found in the way NTP handled rate limiting. An attacker able to send a large number of crafted requests to an NTP server could trigger the rate limiting on that server, and prevent clients from getting a usable reply from the server.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1228
6203	CVE-2015-7704	MEDIUM	High	configuration directives "pidfile" and "driftfile" should only be allowed locally.	ntp	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1227
6204	CVE-2015-7703	MEDIUM	High	configuration directives "pidfile" and "driftfile" should only be allowed locally.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1226
6205	CVE-2015-7702	MEDIUM	Medium	It was found that the fix for CVE-2014-9750 was incomplete: three issues were found in the value length checks in ntp_crypto.c, where a packet with particular autokey operations that contained malicious data was not always being completely validated. Receipt of these packets can cause ntpd to crash.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1225
6206	CVE-2015-7701	HIGH	High	A memory leak flaw was found in ntpd's CRYPTO_ASSOC. If ntpd is configured to use autokey authentication, an attacker could send packets to ntpd that would, after several days of ongoing attack, cause it to run out of memory.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1230
6207	CVE-2015-7697	Medium		Info-ZIP UnZip 6.0 allows remote attackers to cause a denial of service (infinite loop) via empty bzip2 data in a ZIP archive.	unzip	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1575
6208	CVE-2015-7696	Medium		Info-ZIP UnZip 6.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly execute arbitrary code via a crafted password-protected ZIP archive, possibly related to an Extra-Field size value.	unzip	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1571
6209	CVE-2015-7692	MEDIUM	High	It was found that the fix for CVE-2014-9750 was incomplete: three issues were found in the value length checks in ntp_crypto.c, where a packet with particular autokey operations that contained malicious data was not always being completely validated. Receipt of these packets can cause ntpd to crash.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1224
6210	CVE-2015-7691	MEDIUM	High	It was found that the fix for CVE-2014-9750 was incomplete: three issues were found in the value length checks in ntp_crypto.c, where a packet with particular autokey operations that contained malicious data was not always being completely validated. Receipt of these packets can cause ntpd to crash.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1223
6211	CVE-2015-7674	Medium		Integer overflow in the pixops_scale_nearest function in pixops/pixops.c in gdk-pixbuf before 2.32.1 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted GIF image file, which triggers a heap-based buffer overflow.	gdk-pixbuf	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1339
6212	CVE-2015-7673	Medium		io-tga.c in gdk-pixbuf before 2.32.0 uses heap memory after its allocation failed, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) and possibly execute arbitrary code via a crafted Truevision TGA (TARGA) file.	gdk-pixbuf	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1321
6213	CVE-2015-7613	Medium		Race condition in the IPC object implementation in the Linux kernel through 4.2.3 allows local users to gain privileges by triggering an ipc_addid call that leads to uid and gid comparisons against uninitialized data, related to msg.c, shm.c, and util.c.	linux	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-223
6214	CVE-2015-7575	MEDIUM	Medium	Mozilla Network Security Services (NSS) before 3.20.2, as used in Mozilla Firefox before 43.0.2 and Firefox ESR 38.x before 38.5.2, does not reject MD5 signatures in Server Key Exchange messages in TLS 1.2 Handshake Protocol traffic, which makes it easier for man-in-the-middle attackers to spoof servers by triggering a collision.	openssl & gnutls & nss	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-89
6215	CVE-2015-7566	MEDIUM	Medium	The clie_5_attach function in drivers/usb/serial/visor.c in the Linux kernel through 4.4.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by inserting a USB device that lacks a bulk-out endpoint.	linux	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-227
6216	CVE-2015-7560	Medium	Medium	The SMB1 implementation in smbd in Samba 3.x and 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6, and 4.4.x before 4.4.0rc4 allows remote authenticated users to modify arbitrary ACLs by using a UNIX SMB1 call to create a symlink, and then using a non-UNIX SMB1 call to write to the ACL content.	samba	Unchanged	8.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-406
6217	CVE-2015-7558	MEDIUM	High	Stack exhaustion due to cyclic dependency causing to crash an application was found in librsvg2 while parsing SVG file by an application linked against libxml2, could cause the application to disclose heap memory contents.	librsvg	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-284
6218	CVE-2015-7557	MEDIUM	High	Out-of-bounds heap read in librsvg2 was found when parsing SVG file	librsvg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-285
6219	CVE-2015-7555	Medium	Medium	Heap-based buffer overflow in giffix.c in giffix in giflib 5.1.1 allows attackers to cause a denial of service (program crash) via crafted image and logical screen width fields in a GIF file.	giflib	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-485
6220	CVE-2015-7554	HIGH	Critical	The _TIFFVGetField function in tif_dir.c in libtiff 4.0.6 allows attackers to cause a denial of service (invalid memory write and crash) or possibly have unspecified other impact via crafted field data in an extension tag in a TIFF image.	libtiff	Unchanged	8.0.0.19	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-110
6221	CVE-2015-7552	High	High	Heap-based buffer overflow in the gdk_pixbuf_flip function in gdk-pixbuf-scale.c in gdk-pixbuf 2.30.x allows remote attackers to cause a denial of service or possibly execute arbitrary code via a crafted BMP file.	gdk-pixbuf	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-503
6222	CVE-2015-7551	Medium	High	The Fiddle::Handle implementation in ext/fiddle/handle.c in Ruby before 2.0.0-p648, 2.1 before 2.1.8, and 2.2 before 2.2.4, as distributed in Apple OS X before 10.11.4 and other products, mishandles tainting, which allows context-dependent attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted string, related to the DL module and the libffi library. NOTE: this vulnerability exists because of a CVE-2009-5147 regression.	ruby	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-389

	A	B	C	D	E	F	G	H	I	J	K	L	M
6223	CVE-2015-7550	MEDIUM	Medium	The keyctl_read_key function in security/keys/keyctl.c in the Linux kernel before 4.3.4 does not properly use a semaphore, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted application that leverages a race condition between keyctl_revoke and keyctl_read calls.	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-239
6224	CVE-2015-7549	LOW	Medium	The MSI-X MMIO support in hw/pci/msix.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (NULL pointer dereference and QEMU process crash) by leveraging failure to define the .write method.	qemu	Unchanged	8.0.0.24	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2474
6225	CVE-2015-7547	Medium	High	Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing dual A/AAAA DNS queries and the libnss_dns.so.2 NSS module.	glibc	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-292
6226	CVE-2015-7545	HIGH	Critical	Some protocols (like git-remote-ext) can execute arbitrary code found in the URL. The URLs that submodules use may come from arbitrary sources (e.g., .gitmodules files in a remote repository), and can hurt those who blindly enable recursive fetch. Restrict the allowed protocols to well known and safe ones.	git	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-286
6227	CVE-2015-7540	Medium	High	The LDAP server in the AD domain controller in Samba 4.x before 4.1.22 does not check return values to ensure successful ASN.1 memory allocation, which allows remote attackers to cause a denial of service (memory consumption and daemon crash) via crafted packets.	samba	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-119
6228	CVE-2015-7515	Medium	Medium	The aiptek_probe function in drivers/input/tablet/aiptek.c in the Linux kernel before 4.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device that lacks endpoints.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-637
6229	CVE-2015-7513	MEDIUM	Medium	arch/x86/kvm/x86.c in the Linux kernel before 4.4 does not reset the PIT counter values during state restoration, which allows guest OS users to cause a denial of service (divide-by-zero error and host OS crash) via a zero value, related to the kvm_vm_ioctl_set_pit and kvm_vm_ioctl_set_pit2 functions.	linux	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-244
6230	CVE-2015-7512	MEDIUM	Critical	Buffer overflow in the pcnet_receive function in hw/net/pcnet.c in QEMU, when a guest NIC has a larger MTU, allows remote attackers to cause a denial of service (guest OS crash) or execute arbitrary code via a large packet.	qemu	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-141
6231	CVE-2015-7511	LOW	Low	A vulnerability was found in a way the ECDH encryption algorithm decrypts data. An attacker with a specialised setup can extract the secret decryption key from a target located in an adjacent room within seconds. This is done by measuring the target's electromagnetic emanations.	libgcrypt	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-296
6232	CVE-2015-7510	HIGH	Critical	Stack-based buffer overflow in the getpwnam and getgrnam functions of the NSS module nss-mymachines in systemd.	systemd	Unchanged	8.0.0.22	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5425
6233	CVE-2015-7509	Medium	Medium	fs/ext4/namei.c in the Linux kernel before 3.7 allows physically proximate attackers to cause a denial of service (system crash) via a crafted no-journal filesystem, a related issue to CVE-2013-2015.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-69
6234	CVE-2015-7504	MEDIUM	High	A heap-based buffer overflow flaw was discovered in the way QEMU's AMD PC-Net II Ethernet Controller emulation received certain packets in loopback mode. A privileged user (with the CAP_SYS_RAWIO capability) inside a guest could use this flaw to crash the host QEMU process (resulting in denial of service) or, potentially, execute arbitrary code with privileges of the host QEMU process.	qemu	Unchanged	8.0.0.3	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-279
6235	CVE-2015-7500	Medium		The xmlParseMisc function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service (out-of-bounds heap read) via unspecified vectors related to incorrect entities boundaries and start tags.	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-59
6236	CVE-2015-7499	Medium		Heap-based buffer overflow in the xmlGROW function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive process memory information via unspecified vectors.	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-58
6237	CVE-2015-7498	Medium		Heap-based buffer overflow in the xmlParseXmlDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service via unspecified vectors related to extracting errors after an encoding conversion failure.	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-66
6238	CVE-2015-7497	MEDIUM		libxml2: Heap-based buffer overflow in xmlDictComputeFastQKey	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2205
6239	CVE-2015-7313	Medium	Medium	LibTIFF allows remote attackers to cause a denial of service (memory consumption and crash) via a crafted tiff file.	tiff	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3732
6240	CVE-2015-7312	Medium		Multiple race conditions in the Advanced Union Filesystem (aufs) aufs3-mmap.patch and aufs4-mmap.patch patches for the Linux kernel 3.x and 4.x allow local users to cause a denial of service (use-after-free and BUG) or possibly gain privileges via a (1) madvise or (2) msync system call, related to mm/madvise.c and mm/msync.c.	linux	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1909
6241	CVE-2015-7295	Medium		hw/virtio/virtio.c in the Virtual Network Device (virtio-net) support in QEMU, when big or mergeable receive buffers are not supported, allows remote attackers to cause a denial of service (guest network consumption) via a flood of jumbo frames on the (1) tuntap or (2) macvtap interface.	qemu	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1581

	A	B	C	D	E	F	G	H	I	J	K	L	M
6242	CVE-2015-7236	Medium	High	Use-after-free vulnerability in xprt_set_caller in rpcb_svc_com.c in rpcbind 0.2.1 and earlier allows remote attackers to cause a denial of service (daemon crash) via crafted packets, involving a PMAP_CALLIT code.CWE-416: Use After Free	rpcbind	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1090
6243	CVE-2015-7183	High		Integer overflow in the PL_ARENA_ALLOCATE implementation in Netscape Portable Runtime (NSPR) in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors.	nspr	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-92
6244	CVE-2015-7182	High	Critical	Heap-based buffer overflow in the ASN.1 decoder in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OCTET STRING data.	nss	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-91
6245	CVE-2015-7181	High		The sec_asn1d_parse_leaf function in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, improperly restricts access to an unspecified data structure, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OCTET STRING data, related to a use-after-poison issue.	nss	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-90
6246	CVE-2015-7116	Medium	Medium	libxml2 in Apple iOS before 9.2, OS X before 10.11.2, and tvOS before 9.1 allows remote attackers to obtain sensitive information or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2015-7115.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-102
6247	CVE-2015-7115	Medium	Medium	libxml2 in Apple iOS before 9.2, OS X before 10.11.2, and tvOS before 9.1 allows remote attackers to obtain sensitive information or cause a denial of service (memory corruption) via a crafted XML document, a different vulnerability than CVE-2015-7116.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-97
6248	CVE-2015-7098	Medium		WebKit in Apple iOS before 9.2, Safari before 9.0.2, and tvOS before 9.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than CVE-2015-7048, CVE-2015-7095, CVE-2015-7096, CVE-2015-7097, CVE-2015-7099, CVE-2015-7100, CVE-2015-7101, CVE-2015-7102, and CVE-2015-7103.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-416
6249	CVE-2015-7096	Medium		WebKit in Apple iOS before 9.2, Safari before 9.0.2, and tvOS before 9.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than CVE-2015-7048, CVE-2015-7095, CVE-2015-7097, CVE-2015-7098, CVE-2015-7099, CVE-2015-7100, CVE-2015-7101, CVE-2015-7102, and CVE-2015-7103.	webkit	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-415
6250	CVE-2015-7082	High		Multiple unspecified vulnerabilities in Git before 2.5.4, as used in Apple Xcode before 7.2, have unknown impact and attack vectors. NOTE: this CVE is associated only with Xcode use cases.	git	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2206
6251	CVE-2015-6941	MEDIUM	Critical	win_useradd, salt-cloud and the Linode driver in salt 2015.5.x before 2015.5.6, and 2015.8.x before 2015.8.1 leak password information in debug logs.	salt	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4961
6252	CVE-2015-6937	High		The __rds_conn_create function in net/rds/connection.c in the Linux kernel through 4.2.3 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by using a socket that was not properly bound.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-225
6253	CVE-2015-6925	Medium	High	wolfSSL (formerly CyaSSL) before 3.6.8 allows remote attackers to cause a denial of service (resource consumption or traffic amplification) via a crafted DTLS cookie in a ClientHello message.	wolfssl	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-168
6254	CVE-2015-6918	LOW	Medium	salt before 2015.5.5 leaks git usernames and passwords to the log.	salt	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5599
6255	CVE-2015-6908	MEDIUM		The ber_get_next function in libraries/liblber/io.c in OpenLDAP 2.4.42 and earlier allows remote attackers to cause a denial of service (reachable assertion and application crash) via crafted BER data, as demonstrated by an attack against slapd.	openldap	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-886
6256	CVE-2015-6855	High		hw/ide/core.c in QEMU does not properly restrict the commands accepted by an ATAPI device, which allows guest users to cause a denial of service or possibly have unspecified other impact via certain IDE commands, as demonstrated by a WIN_READ_NATIVE_MAX command to an empty drive, which triggers a divide-by-zero error and instance crash.	qemu	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1577
6257	CVE-2015-6838	Medium	High	The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6837.CWE-476: NULL Pointer Dereference	php & libxml2	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-748

	A	B	C	D	E	F	G	H	I	J	K	L	M
6258	CVE-2015-6837	Medium	High	The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation during initial error checking, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6838.CWE-476: NULL Pointer Dereference	php & libxml2	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-775
6259	CVE-2015-6836	High	High	The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage headers, which allows remote attackers to execute arbitrary code via crafted serialized data that triggers a type confusion in the serialize_function_call function.CWE-843: Access of Resource Using Incompatible Type ('Type Confusion')	php	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-196
6260	CVE-2015-6835	High	Critical	The session deserializer in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 mishandles multiple php_var_unserialize calls, which allow remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted session content.CWE-416: Use After Free	php	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-710
6261	CVE-2015-6834	High	Critical	Multiple use-after-free vulnerabilities in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 allow remote attackers to execute arbitrary code via vectors related to (1) the Serializable interface, (2) the SplObjectStorage class, and (3) the SplDoublyLinkedList class, which are mishandled during unserialization.CWE-502: Deserialization of Untrusted Data	php	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-746
6262	CVE-2015-6833	Medium	High	Directory traversal vulnerability in the PharData class in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to write to arbitrary files via a .. (dot dot) in a ZIP archive entry that is mishandled during an extractTo call.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-198
6263	CVE-2015-6832	High	High	Use-after-free vulnerability in the SPL unserialize implementation in ext/spl/spl_array.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to execute arbitrary code via crafted serialized data that triggers misuse of an array field.CWE-416: Use After Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-193
6264	CVE-2015-6831	High	High	Multiple use-after-free vulnerabilities in SPL in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allow remote attackers to execute arbitrary code via vectors involving (1) ArrayObject, (2) SplObjectStorage, and (3) SplDoublyLinkedList, which are mishandled during unserialization.CWE-416: Use After Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-156
6265	CVE-2015-6830	MEDIUM		libraries/plugins/auth/AuthenticationCookie.class.php in phpMyAdmin 4.3.x before 4.3.13.2 and 4.4.x before 4.4.14.1 allows remote attackers to bypass a multiple-reCaptcha protection mechanism against brute-force credential guessing by providing a correct response to a single reCaptcha.	phpMyAdmin	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-869
6266	CVE-2015-6826	High		The ff_rv34_decode_init_thread_copy function in libavcodec/rv34.c in FFmpeg before 2.7.2 does not initialize certain structure members, which allows remote attackers to cause a denial of service (invalid pointer access) or possibly have unspecified other impact via crafted (1) RV30 or (2) RV40 RealVideo data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-875
6267	CVE-2015-6825	High		The ff_frame_thread_init function in libavcodec/pthread_frame.c in FFmpeg before 2.7.2 mishandles certain memory-allocation failures, which allows remote attackers to cause a denial of service (invalid pointer access) or possibly have unspecified other impact via a crafted file, as demonstrated by an AVI file.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-877
6268	CVE-2015-6824	High		The sws_init_context function in libswscale/utils.c in FFmpeg before 2.7.2 does not initialize certain pixbuf data structures, which allows remote attackers to cause a denial of service (segmentation violation) or possibly have unspecified other impact via crafted video data.	gst-ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-882
6269	CVE-2015-6823	High		The allocate_buffers function in libavcodec/alac.c in FFmpeg before 2.7.2 does not initialize certain context data, which allows remote attackers to cause a denial of service (segmentation violation) or possibly have unspecified other impact via crafted Apple Lossless Audio Codec (ALAC) data.	gst-ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-870
6270	CVE-2015-6822	High		The destroy_buffers function in libavcodec/sanm.c in FFmpeg before 2.7.2 does not properly maintain height and width values in the video context, which allows remote attackers to cause a denial of service (segmentation violation and application crash) or possibly have unspecified other impact via crafted LucasArts Smush video data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-874
6271	CVE-2015-6821	High		The ff_mpv_common_init function in libavcodec/mpegvideo.c in FFmpeg before 2.7.2 does not properly maintain the encoding context, which allows remote attackers to cause a denial of service (invalid pointer access) or possibly have unspecified other impact via crafted MPEG data.	gst-ffmpeg	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN8-871

	A	B	C	D	E	F	G	H	I	J	K	L	M
6272	CVE-2015-6820	High		The ff_sbr_apply function in libavcodec/aacsbr.c in FFmpeg before 2.7.2 does not check for a matching AAC frame syntax element before proceeding with Spectral Band Replication calculations, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted AAC data.	gst-ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-876
6273	CVE-2015-6819	High		Multiple integer underflows in the ff_mjpeg_decode_frame function in libavcodec/mjpegdec.c in FFmpeg before 2.7.2 allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted MJPEG data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-885
6274	CVE-2015-6818	High		The decode_ihdr_chunk function in libavcodec/pngdec.c in FFmpeg before 2.7.2 does not enforce uniqueness of the IHDR (aka image header) chunk in a PNG image, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via a crafted image with two or more of these chunks.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-873
6275	CVE-2015-6815	LOW	LOW	The process_tx_desc function in hw/net/e1000.c in QEMU before 2.4.0.1 does not properly process transmit descriptor data when sending a network packet, which allows attackers to cause a denial of service (infinite loop and guest crash) via unspecified vectors.	qemu	Unchanged	8.0.0.33	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3991
6276	CVE-2015-6806	Medium		The MScrollV function in ansi.c in GNU screen 4.3.1 and earlier does not properly limit recursion, which allows remote attackers to cause a denial of service (stack consumption) via an escape sequence with a large repeat count value.	screen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1087
6277	CVE-2015-6761	Medium		The update_dimensions function in libavcodec/vp8.c in FFmpeg through 2.8.1, as used in Google Chrome before 46.0.2490.71 and other products, relies on a coefficient-partition count during multi-threaded operation, which allows remote attackers to cause a denial of service (race condition and memory corruption) or possibly have unspecified other impact via a crafted WebM file.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1336
6278	CVE-2015-6749	Medium		Buffer overflow in the aiff_open function in oggenc/audio.c in vorbis-tools 1.4.0 and earlier allows remote attackers to cause a denial of service (crash) via a crafted AIFF file.	Vorbis-tools	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-974
6279	CVE-2015-6607	Medium		SQLite before 3.8.9, as used in Android before 5.1.1 LMY48T, allows attackers to gain privileges via a crafted application, aka internal bug 20099586.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1086
6280	CVE-2015-6581	High		Double free vulnerability in the opj_j2k_copy_default_tcp_and_create_tcd function in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 45.0.2454.85, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by triggering a memory-allocation failure.CWE-415: Double Free	openjpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-890
6281	CVE-2015-6565	High		sshd in OpenSSH 6.8 and 6.9 uses world-writable permissions for TTY devices, which allows local users to cause a denial of service (terminal disruption) or possibly have unspecified other impact by writing to a device, as demonstrated by writing an escape sequence.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-784
6282	CVE-2015-6564	Medium		Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-777
6283	CVE-2015-6563	Low		The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.	openssh	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-785
6284	CVE-2015-6527	High	High	The php_str_replace_in_subject function in ext/standard/string.c in PHP 7.x before 7.0.0 allows remote attackers to execute arbitrary code via a crafted value in the third argument to the str_ireplace function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-194
6285	CVE-2015-6526	Medium		The perf_callchain_user_64 function in arch/powerpc/perf/callchain.c in the Linux kernel before 4.0.2 on ppc64 platforms allows local users to cause a denial of service (infinite loop) via a deep 64-bit userspace backtrace.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-200
6286	CVE-2015-6525	High		Multiple integer overflows in the evbuffer API in Libevent 2.0.x before 2.0.22 and 2.1.x before 2.1.5-beta allow context-dependent attackers to cause a denial of service or possibly have other unspecified impact via insanely large inputs to the (1) evbuffer_add, (2) evbuffer_prepend, (3) evbuffer_expand, (4) exbuffer_reserve_space, or (5) evbuffer_read function, which triggers a heap-based buffer overflow or an infinite loop. NOTE: this identifier was SPLIT from CVE-2014-6272 per ADT3 due to different affected versions.	libevent	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-790
6287	CVE-2015-6496	Medium		conntrackd in conntrack-tools 1.4.2 and earlier does not ensure that the optional kernel modules are loaded before using them, which allows remote attackers to cause a denial of service (crash) via a (1) DCCP, (2) SCTP, or (3) ICMPv6 packet.	conntrack-tools	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-776

	A	B	C	D	E	F	G	H	I	J	K	L	M
6288	CVE-2015-6386	Medium		The passthrough FTP feature on Cisco Web Security Appliance (WSA) devices with software 8.0.7-142 and 8.5.1-021 allows remote attackers to cause a denial of service (CPU consumption) via FTP sessions in which the control connection is ended after data transfer, aka Bug ID CSCut94150.	WRLinux doesn't ship WSA	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2203
6289	CVE-2015-6252	Low		The vhost_dev_ioctl function in drivers/vhost/vhost.c in the Linux kernel before 4.1.5 allows local users to cause a denial of service (memory consumption) via a VHOST_SET_LOG_FD ioctl call that triggers permanent file-descriptor allocation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-222
6290	CVE-2015-6251	Medium		Double free vulnerability in GnuTLS before 3.3.17 and 3.4.x before 3.4.4 allows remote attackers to cause a denial of service via a long DistinguishedName (DN) entry in a certificate.CWE-415: Double Free	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-771
6291	CVE-2015-6249	Medium		The dissect_wccp2r1_address_table_info function in epan/dissectors/packet-wccp.c in the WCCP dissector in Wireshark 1.12.x before 1.12.7 does not prevent the conflicting use of a table for both IPv4 and IPv6 addresses, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-788
6292	CVE-2015-6248	Medium		The ptvcursor_add function in the ptvcursor implementation in epan/proto.c in Wireshark 1.12.x before 1.12.7 does not check whether the expected amount of data is available, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-779
6293	CVE-2015-6247	Medium		The dissect_openflow_tablemod_v5 function in epan/dissectors/packet-openflow_v5.c in the OpenFlow dissector in Wireshark 1.12.x before 1.12.7 does not validate a certain offset value, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	wireshark	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-783
6294	CVE-2015-6246	Medium		The dissect_wa_payload function in epan/dissectors/packet-waveagent.c in the WaveAgent dissector in Wireshark 1.12.x before 1.12.7 mishandles large tag values, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-773
6295	CVE-2015-6245	Medium		epan/dissectors/packet-gsm_rlcmac.c in the GSM RLC/MAC dissector in Wireshark 1.12.x before 1.12.7 uses incorrect integer data types, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	wireshark	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-778
6296	CVE-2015-6244	Medium		The dissect_zbee_secure function in epan/dissectors/packet-zbee-security.c in the ZigBee dissector in Wireshark 1.12.x before 1.12.7 improperly relies on length fields contained in packet data, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-781
6297	CVE-2015-6243	Medium		The dissector-table implementation in epan/packet.c in Wireshark 1.12.x before 1.12.7 mishandles table searches for empty strings, which allows remote attackers to cause a denial of service (application crash) via a crafted packet, related to the (1) dissector_get_string_handle and (2) dissector_get_default_string_handle functions.	wireshark	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-770
6298	CVE-2015-6242	Medium		The wmem_block_split_free_chunk function in epan/wmem/wmem_allocator_block.c in the wmem block allocator in the memory manager in Wireshark 1.12.x before 1.12.7 does not properly consider a certain case of multiple realloc operations that restore a memory chunk to its original size, which allows remote attackers to cause a denial of service (incorrect free operation and application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-769
6299	CVE-2015-6241	Medium		The proto_tree_add_bytes_item function in epan/proto.c in the protocol-tree implementation in Wireshark 1.12.x before 1.12.7 does not properly terminate a data structure after a failure to locate a number within a string, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-786
6300	CVE-2015-5986	High		openpgpkey_61.c in named in ISC BIND 9.9.7 before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a crafted DNS response.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-883
6301	CVE-2015-5895	High		Multiple unspecified vulnerabilities in SQLite before 3.8.10.2, as used in Apple iOS before 9, have unknown impact and attack vectors.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-971
6302	CVE-2015-5745			Qemu emulator built with the virtio-serial vmchannel support is vulnerable to a buffer overflow issue. It could occur while exchanging virtio control messages between guest & the host.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4062
6303	CVE-2015-5740	HIGH	Critical	The net/http library in net/http/transfer.go in Go before 1.4.3 does not properly parse HTTP headers, which allows remote attackers to conduct HTTP request smuggling attacks via a request with two Content-length headers.	go	Unchanged	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5710
6304	CVE-2015-5739	HIGH	Critical	The net/http library in net/textproto/reader.go in Go before 1.4.3 does not properly parse HTTP header keys, which allows remote attackers to conduct HTTP request smuggling attacks via a space instead of a hyphen, as demonstrated by Content Length instead of Content-Length.	go	Unchanged	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5709
6305	CVE-2015-5738	HIGH	High	libgcrypt contains an unspecified flaw related to the verification of created RSA signatures, which may allow an attacker to gain access to private key information. No further details have been provided.	libgcrypt	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-88

	A	B	C	D	E	F	G	H	I	J	K	L	M
6306	CVE-2015-5722	High		buffer.c in named in ISC BIND 9.x before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) by creating a zone containing a malformed DNSSEC key and issuing a query for a name in that zone.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-861
6307	CVE-2015-5707	Medium		Integer overflow in the sg_start_req function in drivers/scsi/sg.c in the Linux kernel 2.6.x through 4.x before 4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large iov_count value in a write request.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-220
6308	CVE-2015-5706	Medium		Use-after-free vulnerability in the path_openat function in fs/namei.c in the Linux kernel 3.x and 4.x before 4.0.4 allows local users to cause a denial of service or possibly have unspecified other impact via O_TMPFILE filesystem operations that leverage a duplicate cleanup operation.CWE-416: Use After Free	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-214
6309	CVE-2015-5697	Low		The get_bitmap_file function in drivers/md/md.c in the Linux kernel before 4.1.6 does not initialize a certain bitmap data structure, which allows local users to obtain sensitive information from kernel memory via a GET_BITMAP_FILE ioctl call.	linux	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-213
6310	CVE-2015-5652	High		Untrusted search path vulnerability in python.exe in Python through 3.5.0 on Windows allows local users to gain privileges via a Trojan horse readline.pyd file in the current working directory. NOTE: the vendor says It was determined that this is a longtime behavior of Python that cannot really be altered at this point.CWE-426: Untrusted Search Path	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1084
6311	CVE-2015-5621	High		The snmp_pdu_parse function in snmp_api.c in net-snmp 5.7.2 and earlier does not remove the varBind variable in a netsnmp_variable_list item when parsing of the SNMP PDU fails, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-747
6312	CVE-2015-5602	High		sudoedit in Sudo before 1.8.15 allows local users to gain privileges via a symlink attack on a file whose full path is defined using multiple wildcards in /etc/sudoers, as demonstrated by /home/*/*/file.txt.	sudo	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1914
6313	CVE-2015-5600	High		The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.	openssh	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-703
6314	CVE-2015-5590	High	High	Stack-based buffer overflow in the phar_fix_filepath function in ext/phar/phar.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value, as demonstrated by mishandling of an e-mail attachment by the imap PHP extension.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-204
6315	CVE-2015-5589	High	Critical	The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-780
6316	CVE-2015-5523	Medium		The ParseValue function in lexer.c in tidy before 4.9.31 allows remote attackers to cause a denial of service (crash) via vectors involving multiple whitespace characters before an empty href, which triggers a large memory allocation.	tidy	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-722
6317	CVE-2015-5522	Medium		Heap-based buffer overflow in the ParseValue function in lexer.c in tidy before 4.9.31 allows remote attackers to cause a denial of service (crash) via vectors involving a command character in an href.	tidy	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-706
6318	CVE-2015-5479	MEDIUM	Medium	The ff_h263_decode_mba function in libavcodec/ituh263dec.c in Libav before 11.5 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a file with crafted dimensions.	libav	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-510
6319	CVE-2015-5477	High		named in ISC BIND 9.x before 9.9.7-P2 and 9.10.x before 9.10.2-P3 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via TKEY queries.	bind	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-657
6320	CVE-2015-5370	MEDIUM	Medium	Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not properly implement the DCE-RPC layer, which allows remote attackers to perform protocol-downgrade attacks, cause a denial of service (application crash or CPU consumption), or possibly execute arbitrary code on a client system via unspecified vectors.	samba	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-488
6321	CVE-2015-5366	MEDIUM		Linux kernel built with the networking support(CONFIG_NET) is vulnerable to an infinite loop issue. It could occur while receiving(recvmsg(2), recvfrom(2)) data over UDP channel, with an incorrect checksum value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-608
6322	CVE-2015-5364	HIGH		An unprivileged user could use this flaw to cause DoS(CVE-2015-5364) to a remote system via specially crafted UDP packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-645
6323	CVE-2015-5352	Medium		The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.	openssh	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-719

	A	B	C	D	E	F	G	H	I	J	K	L	M
6324	CVE-2015-5343	High	High	Integer overflow in util.c in mod_dav_svn in Apache Subversion 1.7.x, 1.8.x before 1.8.15, and 1.9.x before 1.9.3 allows remote authenticated users to cause a denial of service (subversion server crash or memory consumption) and possibly execute arbitrary code via a skel-encoded request body, which triggers an out-of-bounds read and heap-based buffer overflow.	subversion	Unchanged	8.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-512
6325	CVE-2015-5330	Medium	High	ldb before 1.1.24, as used in the AD LDAP server in Samba 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, mishandles string lengths, which allows remote attackers to obtain sensitive information from daemon heap memory by sending crafted packets and then reading (1) an error message or (2) a database value.	samba	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-95
6326	CVE-2015-5327	MEDIUM	Medium	Out-of-bounds memory read in the x509_decode_time function in x509_cert_parser.c in Linux kernels 4.3-rc1 and after.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5439
6327	CVE-2015-5316			The eap_pwd_perform_confirm_exchange function in eap_peer/eap_pwd.c in wpa_supplicant 2.x before 2.6, when EAP-pwd is enabled in a network configuration profile, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an EAP-pwd Confirm message followed by the Identity exchange.	wpa_supplicant	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3322
6328	CVE-2015-5315			The eap_pwd_process function in eap_peer/eap_pwd.c in wpa_supplicant 2.x before 2.6 does not validate that the reassembly buffer is large enough for the final fragment when EAP-pwd is enabled in a network configuration profile, which allows remote attackers to cause a denial of service (process termination) via a large final fragment in an EAP-pwd message.	wpa_supplicant	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3335
6329	CVE-2015-5314			The eap_pwd_process function in eap_server/eap_server_pwd.c in hostapd 2.x before 2.6 does not validate that the reassembly buffer is large enough for the final fragment when used with (1) an internal EAP server or (2) a RADIUS server and EAP-pwd is enabled in a runtime configuration, which allows remote attackers to cause a denial of service (process termination) via a large final fragment in an EAP-pwd message.	hostapd	Unchanged	8.0.0.26	9.0.0.16	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-3436
6330	CVE-2015-5313	LOW	Low	Directory traversal vulnerability in the virStorageBackendFileSystemVolCreate function in storage/storage_backend_fs.c in libvirt, when fine-grained Access Control Lists (ACL) are in effect, allows local users with storage_vol:create ACL but not domain:write permission to write to arbitrary files via a .. (dot dot) in a volume name.	libvirt	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-427
6331	CVE-2015-5312	HIGH		libxml2: CPU exhaustion when processing specially crafted XML input	libxml2	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2219
6332	CVE-2015-5307	Medium		The KVM subsystem in the Linux kernel through 4.2.6, and Xen 4.3.x through 4.6.x, allows guest OS users to cause a denial of service (host OS panic or hang) by triggering many #AC (aka Alignment Check) exceptions, related to svm.c and vmx.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1918
6333	CVE-2015-5300	MEDIUM	High	It was found that ntpd did not correctly implement the threshold limitation for the '-g' option, which is used to set the time without any restrictions. A man-in-the-middle attacker able to intercept NTP traffic between a connecting client and an NTP server could use this flaw to force that client to make multiple steps larger than the panic threshold, effectively changing the time to an arbitrary value at any time.	ntp	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-342
6334	CVE-2015-5299	Medium	Medium	The shadow_copy2_get_shadow_copy_data function in modules/vfs_shadow_copy2.c in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3 does not verify that the DIRECTORY_LIST access right has been granted, which allows remote attackers to access snapshots by visiting a shadow copy directory.	samba	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-128
6335	CVE-2015-5297	High	CRITICAL	An integer overflow issue has been reported in the general_composite_rect() function in pixman prior to version 0.32.8. An attacker could exploit this issue to cause an application using pixman to crash or, potentially, execute arbitrary code.	pixman	Unchanged	8.0.0.31	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4610
6336	CVE-2015-5296	Medium	Medium	Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3 supports connections that are encrypted but unsigned, which allows man-in-the-middle attackers to conduct encrypted-to-unencrypted downgrade attacks by modifying the client-server data stream, related to clidfs.c, libsmb_server.c, and smbXcli_base.c.	samba	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-93
6337	CVE-2015-5291	Medium		Heap-based buffer overflow in PolarSSL 1.x before 1.2.17 and ARM mbed TLS (formerly PolarSSL) 1.3.x before 1.3.14 and 2.x before 2.1.2 allows remote SSL servers to cause a denial of service (client crash) and possibly execute arbitrary code via a long hostname to the server name indication (SNI) extension, which is not properly handled when creating a ClientHello message. NOTE: this identifier has been SPLIT per ADT3 due to different affected version ranges. See CVE-2015-8036 for the session ticket issue that was introduced in 1.3.0.	polarssl	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1573
6338	CVE-2015-5289	Medium		Multiple stack-based buffer overflows in json parsing in PostgreSQL before 9.3.x before 9.3.10 and 9.4.x before 9.4.5 allow attackers to cause a denial of service (server crash) via unspecified vectors, which are not properly handled in (1) json or (2) jsonb values.	postgresql	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1340
6339	CVE-2015-5288	Medium		The crypt function in contrib/pgcrypto in PostgreSQL before 9.0.23, 9.1.x before 9.1.19, 9.2.x before 9.2.14, 9.3.x before 9.3.10, and 9.4.x before 9.4.5 allows attackers to cause a denial of service (server crash) or read arbitrary server memory via a too-short salt.	postgresql	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1353

	A	B	C	D	E	F	G	H	I	J	K	L	M
6340	CVE-2015-5283	Medium		The sctp_init function in net/sctp/protocol.c in the Linux kernel before 4.2.3 has an incorrect sequence of protocol-initialization steps, which allows local users to cause a denial of service (panic or memory corruption) by creating SCTP sockets before all of the steps have finished.	linux	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-219
6341	CVE-2015-5281	Low		The grub2 package before 2.02-0.29 in Red Hat Enterprise Linux (RHEL) 7, when used on UEFI systems, allows local users to bypass intended Secure Boot restrictions and execute non-verified code via a crafted (1) multiboot or (2) multiboot2 module in the configuration file or physically proximate attackers to bypass intended Secure Boot restrictions and execute non-verified code via the (3) boot menu.	grub2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1927
6342	CVE-2015-5279	High		Heap-based buffer overflow in the ne2000_receive function in hw/net/ne2000.c in QEMU before 2.4.0.1 allows guest OS users to cause a denial of service (instance crash) or possibly execute arbitrary code via vectors related to receiving packets.	qemu	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1092
6343	CVE-2015-5278			A flaw was found where a QEMU emulator built with NE2000 NIC emulation support was vulnerable to an infinite loop issue that occurred when receiving packets over the network. A privileged user inside a guest could use this flaw to crash the QEMU instance, resulting in a denial of service as per CVE-2015-5278 , impacts qemu < 2.4.3	qemu	Unchanged	8.0.0.27	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4082
6344	CVE-2015-5277	High		The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) before 2.20 might allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS files database.	glibc	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-61
6345	CVE-2015-5276	Medium		The std::random_device class in libstdc++ in the GNU Compiler Collection (aka GCC) before 4.9.4 does not properly handle short reads from blocking sources, which makes it easier for context-dependent attackers to predict the random values via unspecified vectors.	gcc	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1915
6346	CVE-2015-5259	High	High	Integer overflow in the read_string function in libsvn_ra_svn/marshal.c in Apache Subversion 1.9.x before 1.9.3 allows remote attackers to execute arbitrary code via an svn:// protocol string, which triggers a heap-based buffer overflow and an out-of-bounds read.	subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-130
6347	CVE-2015-5257	Medium		drivers/usb/serial/whiteheat.c in the Linux kernel before 4.2.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a crafted USB device. NOTE: this ID was incorrectly used for an Apache Cordova issue that has the correct ID of CVE-2015-8320.CWE-476: NULL Pointer Dereference	linux	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1912
6348	CVE-2015-5252	Medium	High	vfs.c in smbd in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, when share names with certain substring relationships exist, allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share.	samba	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-136
6349	CVE-2015-5247	Medium	Medium	The virStorageVolCreateXML API in libvirt 1.2.14 through 1.2.19 allows remote authenticated users with a read-write connection to cause a denial of service (libvirtd crash) by triggering a failed unlink after creating a volume on a root_squash NFS pool.	libvirt	Unchanged	8.0.0.5	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-492
6350	CVE-2015-5239	MEDIUM	MEDIUM	Integer overflow in the VNC display driver in QEMU before 2.1.0 allows attachers to cause a denial of service (process crash) via a CLIENT_CUT_TEXT message, which triggers an infinite loop.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10.20.12.0	LIN1019-4051
6351	CVE-2015-5237	MEDIUM	High	protobuf allows remote authenticated attackers to cause a heap-based buffer overflow.	protobuf	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5440
6352	CVE-2015-5231	Low	Medium	The service daemon in CRIU does not properly restrict access to non-dumpable processes, which allows local users to obtain sensitive information via (1) process dumps or (2) ptrace access.	criu	Unchanged	Vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-848
6353	CVE-2015-5229	MEDIUM	High	It was discovered that the calloc implementation in glibc could return memory areas which contain non-zero bytes. This could result in unexpected application behavior such as hangs or crashes.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-332
6354	CVE-2015-5228	High	High	The service daemon in CRIU creates log and dump files insecurely, which allows local users to create arbitrary files and take ownership of existing files via unspecified vectors related to a directory path.	criu	Unchanged	Vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-836
6355	CVE-2015-5225	High		Buffer overflow in the vnc_refresh_server_surface function in the VNC display driver in QEMU before 2.4.0.1 allows guest users to cause a denial of service (heap memory corruption and process crash) or possibly execute arbitrary code on the host via unspecified vectors, related to refreshing the server display surface.	qemu	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1572
6356	CVE-2015-5224	HIGH	Critical	The mkostemp function in login-utils in util-linux when used incorrectly allows remote attackers to cause file name collision and possibly other attacks.	util-linux	Unchanged	8.0.0.22	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5122
6357	CVE-2015-5221	MEDIUM	Medium	Use-after-free vulnerability in the mif_process_cmpt function in libjasper/mif/mif_cod.c in the JasPer JPEG-2000 library before 1.900.2 allows remote attackers to cause a denial of service (crash) via a crafted JPEG 2000 image file.	jasper	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4772
6358	CVE-2015-5219	MEDIUM	High	The ULOGTOD function in ntp.d in SNTP before 4.2.7p366 does not properly perform type conversions from a precision value to a double, which allows remote attackers to cause a denial of service (infinite loop) via a crafted NTP packet.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4859
6359	CVE-2015-5218	Low		Buffer overflow in text-utils/colcrt.c in colcrt in util-linux before 2.27 allows local users to cause a denial of service (crash) via a crafted file, related to the page global variable.	util-linux	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1569

	A	B	C	D	E	F	G	H	I	J	K	L	M
6360	CVE-2015-5203	MEDIUM	Medium	A double free flaw was found in the way JasPer's jasper_image_stop_load() function parsed certain JPEG 2000 image files. A specially crafted file could cause an application using JasPer to crash.	jasper	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-448
6361	CVE-2015-5195	MEDIUM	High	ntp_openssl.m4 in ntpd in NTP before 4.2.7p112 allows remote attackers to cause a denial of service (segmentation fault) via a crafted statistics or filegen configuration command that is not enabled during compilation.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4860
6362	CVE-2015-5194	MEDIUM	High	The log_config_command function in ntp_parser.y in ntpd in NTP before 4.2.7p42 allows remote attackers to cause a denial of service (ntpd crash) via crafted logconfig commands.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4838
6363	CVE-2015-5186	MEDIUM	Medium	Audit before 2.4.4 in Linux does not sanitize escape characters in filenames.	audit	Unchanged	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5289
6364	CVE-2015-5185	Medium		The lookupProviders function in providerMgr.c in sblim-sfcb 1.3.4 and 1.3.18 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty className in a packet.CWE-476: NULL Pointer Dereference	sblim-sfcb	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1104
6365	CVE-2015-5180	MEDIUM	High	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash).	glibc	Unchanged	8.0.0.20	9.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4527
6366	CVE-2015-5166	High		Use-after-free vulnerability in QEMU in Xen 4.5.x and earlier does not completely unplug emulated block devices, which allows local HVM guest users to gain privileges by unplugging a block device twice.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-715
6367	CVE-2015-5165	Medium		The C+ mode offload emulation in the RTL8139 network card device model in QEMU, as used in Xen 4.5.x and earlier, allows remote attackers to read process heap memory via unspecified vectors.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-710
6368	CVE-2015-5163	Low		The import task action in OpenStack Image Service (Glance) 2015.1.x before 2015.1.2 (kilo), when using the V2 API, allows remote authenticated users to read arbitrary files via a crafted backing file for a qcow2 image.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2528
6369	CVE-2015-5160			libvirt before 2.2 includes Ceph credentials on the qemu command line when using RADOS Block Device (aka RBD), which allows local users to obtain sensitive information via a process listing.	libvirt	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4610
6370	CVE-2015-5158	MEDIUM	Medium	Stack-based buffer overflow in hw/scsi/scsi-bus.c in QEMU, when built with SCSI-device emulation support, allows guest OS users with CAP_SYS_RAWIO permissions to cause a denial of service (instance crash) via an invalid opcode in a SCSI command descriptor block.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-442
6371	CVE-2015-5157	High		arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform mishandles IRET faults in processing NMIs that occurred during userspace execution, which might allow local users to gain privileges by triggering an NMI.	linux	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-207
6372	CVE-2015-5156	Medium		The virtnet_probe function in drivers/net/virtio_net.c in the Linux kernel before 4.2 attempts to support a FRAGLIST feature without proper memory allocation, which allows guest OS users to cause a denial of service (buffer overflow and memory corruption) via a crafted sequence of fragmented packets.	linux	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-226
6373	CVE-2015-5154	High		Heap-based buffer overflow in the IDE subsystem in QEMU, as used in Xen 4.5.x and earlier, when the container has a CDROM drive enabled, allows local guest users to execute arbitrary code on the host via unspecified ATAPI commands.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-714
6374	CVE-2015-5146	LOW	Medium	Under limited and specific circumstances an attacker can send a crafted packet to cause a vulnerable ntpd instance to crash. This requires each of the following to be true:	ntp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN8-528
6375	CVE-2015-5073	MEDIUM	Critical	PCRE library is prone to a vulnerability which leads to Heap Overflow.During subpattern calculation of a malformed regular expression, an offset that is used as an array index is fully controlled and can be large enough so that unexpected heap memory regions are accessed. One could at least exploit this issue to read objects nearby of the affected application's memory. Such information disclosure may also be used to bypass memory protection method such as ASLR.	pcre	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-805
6376	CVE-2015-4913	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via vectors related to Server : DML, a different vulnerability than CVE-2015-4858.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1327
6377	CVE-2015-4910	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1344
6378	CVE-2015-4905	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via vectors related to Server : DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1334
6379	CVE-2015-4904	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to libmysqld.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1362
6380	CVE-2015-4895	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1317
6381	CVE-2015-4890	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1323
6382	CVE-2015-4879	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.44 and earlier, and 5.6.25 and earlier, allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1328

	A	B	C	D	E	F	G	H	I	J	K	L	M
6383	CVE-2015-4870	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Parser.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1349
6384	CVE-2015-4866	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1359
6385	CVE-2015-4864	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server : Security : Privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1354
6386	CVE-2015-4862	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1331
6387	CVE-2015-4861	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1333
6388	CVE-2015-4858	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2015-4913.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1361
6389	CVE-2015-4836	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : SP.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1360
6390	CVE-2015-4833	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1322
6391	CVE-2015-4830	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server : Security : Privileges.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1337
6392	CVE-2015-4826	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect confidentiality via unknown vectors related to Server : Types.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1325
6393	CVE-2015-4819	High		Unspecified vulnerability in Oracle MySQL Server 5.5.44 and earlier, and 5.6.25 and earlier, allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Client programs.Per LINK: The CVSS score is 7.2 if the Utility runs with admin or root privileges. The score would be 4.6 if the Utility runs with non-admin privileges and the impact on Confidentiality, Integrity and Availability would be Partial+.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1326
6394	CVE-2015-4816	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.44 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1351
6395	CVE-2015-4815	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via vectors related to Server : DDL.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1345
6396	CVE-2015-4807	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier, when running on Windows, allows remote authenticated users to affect availability via unknown vectors related to Server : Query Cache.This issue impacts the Windows platform only.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1318
6397	CVE-2015-4802	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition, a different vulnerability than CVE-2015-4792.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1335
6398	CVE-2015-4800	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1346
6399	CVE-2015-4792	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition, a different vulnerability than CVE-2015-4802.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1348
6400	CVE-2015-4791	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.This issue impacts the Windows platform only.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1320
6401	CVE-2015-4772	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-664
6402	CVE-2015-4771	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to RBR.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-662
6403	CVE-2015-4769	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Firewall, a different vulnerability than CVE-2015-4767.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-666
6404	CVE-2015-4767	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Firewall, a different vulnerability than CVE-2015-4769.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-661

	A	B	C	D	E	F	G	H	I	J	K	L	M
6405	CVE-2015-4766	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows local users to affect availability via unknown vectors related to Server : Security : Firewall.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1350
6406	CVE-2015-4761	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-670
6407	CVE-2015-4757	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier and 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-647
6408	CVE-2015-4756	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-663
6409	CVE-2015-4752	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to Server : I_S.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-649
6410	CVE-2015-4737	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier, and 5.6.23 and earlier, allows remote authenticated users to affect confidentiality via unknown vectors related to Server : Pluggable Auth.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-667
6411	CVE-2015-4730	Medium		Unspecified vulnerability in Oracle MySQL 5.6.20 and earlier allows remote authenticated users to affect availability via unknown vectors related to Types.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1343
6412	CVE-2015-4700	Medium		The bpf_int_jit_compile function in arch/x86/net/bpf_jit_comp.c in the Linux kernel before 4.0.6 allows local users to cause a denial of service (system crash) by creating a packet filter and then loading crafted BPF instructions that trigger late convergence by the JIT compiler.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-208
6413	CVE-2015-4692	Medium		The kvm_apic_has_events function in arch/x86/kvm/lapic.h in the Linux kernel through 4.1.3 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by leveraging /dev/kvm access for an ioctl call.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-671
6414	CVE-2015-4680	MEDIUM	High	FreeRADIUS 2.2.x before 2.2.8 and 3.0.x before 3.0.9 does not properly check revocation of intermediate CA certificates.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3942
6415	CVE-2015-4652	Medium		epan/dissectors/packet-gsm_a_dtap.c in the GSM DTAP dissector in Wireshark 1.12.x before 1.12.6 does not properly validate digit characters, which allows remote attackers to cause a denial of service (application crash) via a crafted packet, related to the de_emerg_num_list and de_bcd_num functions.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-659
6416	CVE-2015-4651	Medium		The dissect_wccp2r1_address_table_info function in epan/dissectors/packet-wccp.c in the WCCP dissector in Wireshark 1.12.x before 1.12.6 does not properly determine whether enough memory is available for storing IP address strings, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-650
6417	CVE-2015-4646	MEDIUM	High	(1) unsquash-1.c, (2) unsquash-2.c, (3) unsquash-3.c, and (4) unsquash-4.c in Squashfs and sasquatch allow remote attackers to cause a denial of service (application crash) via a crafted input.	squashfs	Unchanged	8.0.0.28	9.0.0.19	10.17.41.13	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4073
6418	CVE-2015-4645	Medium	Medium	Integer overflow in the read_fragment_table_4 function in unsquash-4.c in Squashfs and sasquatch allows remote attackers to cause a denial of service (application crash) via a crafted input, which triggers a stack-based buffer overflow.	squashfs-tools	Unchanged	8.0.0.18	9.0.0.7	10.17.41.3	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-3665
6419	CVE-2015-4644	Medium	High	The php_pgsql_meta_data function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not validate token extraction for table names, which might allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1352.CWE-476: NULL Pointer Dereference	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-751
6420	CVE-2015-4643	High	Critical	Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4022.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-733
6421	CVE-2015-4642	High	Critical	The escapeshellarg function in ext/standard/exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-726
6422	CVE-2015-4625	Medium		Integer overflow in the authentication_agent_new_cookie function in PolicyKit (aka polkit) before 0.113 allows local users to gain privileges by creating a large number of connections, which triggers the issuance of a duplicate cookie value.	polkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1355
6423	CVE-2015-4620	High		name.c in named in ISC BIND 9.7.x through 9.9.x before 9.9.7-P1 and 9.10.x before 9.10.2-P2, when configured as a recursive resolver with DNSSEC validation, allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) by constructing crafted zone data and then making a query for a name in that zone.	bind	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-601

	A	B	C	D	E	F	G	H	I	J	K	L	M
6424	CVE-2015-4605	Medium	High	The mcopy function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly restrict a certain offset value, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a Python script text executable rule.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-719
6425	CVE-2015-4604	Medium	High	The mget function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly maintain a certain pointer relationship, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a Python script text executable rule.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-735
6426	CVE-2015-4603	High	Critical	The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a type confusion issue.Access of Resource Using Incompatible Type ('Type Confusion')	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-784
6427	CVE-2015-4602	High	Critical	The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a type confusion issue.Access of Resource Using Incompatible Type ('Type Confusion')	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-709
6428	CVE-2015-4601	High	Critical	PHP before 5.6.7 might allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to type confusion issues in (1) ext/soap/php_encoding.c, (2) ext/soap/php_http.c, and (3) ext/soap/soap.c, a different issue than CVE-2015-4600.Access of Resource Using Incompatible Type ('Type Confusion')	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-765
6429	CVE-2015-4600	High	Critical	The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to type confusion issues in the (1) SoapClient::__getLastRequest, (2) SoapClient::__getLastResponse, (3) SoapClient::__getLastRequestHeaders, (4) SoapClient::__getLastResponseHeaders, (5) SoapClient::__getCookies, and (6) SoapClient::__setCookie methods.Access of Resource Using Incompatible Type ('Type Confusion')	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-778
6430	CVE-2015-4599	High	Critical	The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a type confusion issue.Access of Resource Using Incompatible Type ('Type Confusion')	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-732
6431	CVE-2015-4598	High	Medium	PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument save method or (2) the GD imagepsloadfont function, as demonstrated by a filename\0.html attack that bypasses an intended configuration in which client users may write to only .html files.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-777
6432	CVE-2015-4506	Medium		Buffer overflow in the vp9_init_context_buffers function in libvpx, as used in Mozilla Firefox before 41.0 and Firefox ESR 38.x before 38.3, allows remote attackers to execute arbitrary code via a crafted VP9 file.	libvpx	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN8-970
6433	CVE-2015-4491	MEDIUM		Integer overflow in the make_filter_table function in pixops/pixops.c in gdk-pixbuf before 2.31.5, as used in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 on Linux, Google Chrome on Linux, and other products, allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow and application crash) via crafted bitmap dimensions that are mishandled during scaling.	gdk-pixbuf	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-707
6434	CVE-2015-4486	HIGH		The decrease_ref_count function in libvpx in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via malformed WebM video data.	libvpx	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-716
6435	CVE-2015-4485	HIGH		Heap-based buffer overflow in the resize_context_buffers function in libvpx in Mozilla Firefox before 40.0 and Firefox ESR 38.x before 38.2 allows remote attackers to execute arbitrary code via malformed WebM video data.	libvpx	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-701

	A	B	C	D	E	F	G	H	I	J	K	L	M
6436	CVE-2015-4178	Medium	Medium	The fs_pin implementation in the Linux kernel before 4.0.5 does not ensure the internal consistency of a certain list data structure, which allows local users to cause a denial of service (system crash) by leveraging user-namespace root access for an MNT_DETACH umount2 system call, related to fs/fs_pin.c and include/linux/fs_pin.h.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-564
6437	CVE-2015-4177	Medium	Medium	The collect_mounts function in fs/namespace.c in the Linux kernel before 4.0.5 does not properly consider that it may execute after a path has been unmounted, which allows local users to cause a denial of service (system crash) by leveraging user-namespace root access for an MNT_DETACH umount2 system call.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-587
6438	CVE-2015-4176	Low	Medium	fs/namespace.c in the Linux kernel before 4.0.2 does not properly support mount connectivity, which allows local users to read arbitrary files by leveraging user-namespace root access for deletion of a file or directory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-655
6439	CVE-2015-4171	Low		strongSwan 4.3.0 through 5.x before 5.3.2 and strongSwan VPN Client before 1.4.6, when using EAP or pre-shared keys for authenticating an IKEv2 connection, does not enforce server authentication restrictions until the entire authentication process is complete, which allows remote servers to obtain credentials by using a valid certificate and then reading the responses.	strongswan	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-433
6440	CVE-2015-4170	Medium	Medium	Race condition in the ldsem_cmpxchg function in drivers/tty/tty_ldsem.c in the Linux kernel before 3.13-rc4-next-20131218 allows local users to cause a denial of service (ldsem_down_read and ldsem_down_write deadlock) by establishing a new tty thread during shutdown of a previous tty thread.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-570
6441	CVE-2015-4167	Medium		The udf_read_inode function in fs/udf/inode.c in the Linux kernel before 3.19.1 does not validate certain length values, which allows local users to cause a denial of service (incorrect data representation or integer overflow, and OOPS) via a crafted UDF filesystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-711
6442	CVE-2015-4148	Medium		The do_soap_call function in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that the uri property is a string, which allows remote attackers to obtain sensitive information by providing crafted serialized data with an int data type, related to a type confusion issue.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-441
6443	CVE-2015-4147	High		The SoapClient::__call method in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that __default_headers is an array, which allows remote attackers to execute arbitrary code by providing crafted serialized data with an unexpected data type, related to a type confusion issue.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-443
6444	CVE-2015-4146	Medium		The EAP-pwd peer implementation in hostapd and wpa_supplicant 1.0 through 2.4 does not clear the L (Length) and M (More) flags before determining if a response should be fragmented, which allows remote attackers to cause a denial of service (crash) via a crafted message.	Hostapd & wpa_supplicant.	Unchanged	8.0.0.0	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-514
6445	CVE-2015-4145	Medium		The EAP-pwd server and peer implementation in hostapd and wpa_supplicant 1.0 through 2.4 does not validate a fragment is already being processed, which allows remote attackers to cause a denial of service (memory leak) via a crafted message.	Hostapd & wpa_supplicant.	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-518
6446	CVE-2015-4144	Medium		The EAP-pwd server and peer implementation in hostapd and wpa_supplicant 1.0 through 2.4 does not validate that a message is long enough to contain the Total-Length field, which allows remote attackers to cause a denial of service (crash) via a crafted message.	Hostapd & wpa_supplicant.	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-512
6447	CVE-2015-4143	Medium		The EAP-pwd server and peer implementation in hostapd and wpa_supplicant 1.0 through 2.4 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted (1) Commit or (2) Confirm message payload.	Hostapd & wpa_supplicant.	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-516
6448	CVE-2015-4142	Medium		Integer underflow in the WMM Action frame parser in hostapd 0.5.5 through 2.4 and wpa_supplicant 0.7.0 through 2.4, when used for AP mode MLME/SME functionality, allows remote attackers to cause a denial of service (crash) via a crafted frame, which triggers an out-of-bounds read.	Hostapd & wpa_supplicant.	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-520
6449	CVE-2015-4141	Medium		The WPS UPnP function in hostapd, when using WPS AP, and wpa_supplicant, when using WPS external registrar (ER), 0.7.0 through 2.4 allows remote attackers to cause a denial of service (crash) via a negative chunk length, which triggers an out-of-bounds read or heap-based buffer overflow.	Hostapd & wpa_supplicant.	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-519
6450	CVE-2015-4116	High	Critical	Use-after-free vulnerability in the spl_ptr_heap_insert function in ext/spl/spl_heap.c in PHP before 5.5.27 and 5.6.x before 5.6.11 allows remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.CWE 416: Use After Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-713
6451	CVE-2015-4106	High		QEMU does not properly restrict write access to the PCI config space for certain PCI pass-through devices, which mighy allow local x86 HVM guests to gain privileges, cause a denial of service (host crash), obtain sensitive information, or possibly have other unspecified impact via unknown vectors.	qemu	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-445

	A	B	C	D	E	F	G	H	I	J	K	L	M
6452	CVE-2015-4100			Puppet Enterprise 3.7.x and 3.8.0 might allow remote authenticated users to manage certificates for arbitrary nodes by leveraging a client certificate trusted by the master, aka a Certificate Authority Reverse Proxy Vulnerability.	puppet	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2924
6453	CVE-2015-4047	HIGH		racoon/gssapi.c in IPsec-Tools 0.8.2 allows remote attackers to cause a denial of service (NULL pointer dereference and IKE daemon crash) via a series of crafted UDP requests.	Ipsec-tools	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-399
6454	CVE-2015-4042	HIGH	CRITICAL	Integer overflow in the keycompare_mb function in sort.c in sort in GNU Coreutils through 8.23 might allow attackers to cause a denial of service (application crash) or possibly have unspecified other impact via long strings.	coreutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-4049
6455	CVE-2015-4041	MEDIUM	HIGH	The keycompare_mb function in sort.c in sort in GNU Coreutils through 8.23 on 64-bit platforms performs a size calculation without considering the number of bytes occupied by multibyte characters, which allows attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via long UTF-8 strings.	coreutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-4050
6456	CVE-2015-4037	Low		The slirp_smb function in net/slirp.c in QEMU 2.3.0 and earlier creates temporary files with predictable names, which allows local users to cause a denial of service (instantiation failure) by creating /tmp/qemu-smb.*-* files before the program.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-789
6457	CVE-2015-4036	High		Array index error in the tcm_vhost_make_tpg function in drivers/vhost/scsi.c in the Linux kernel before 4.0 might allow guest OS users to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted VHOST_SCSI_SET_ENDPOINT ioctl call. NOTE: the affected function was renamed to vhost_scsi_make_tpg before the vulnerability was announced.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-204
6458	CVE-2015-4026	High		The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-453
6459	CVE-2015-4025	High		PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-446
6460	CVE-2015-4024	Medium		Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/rfc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-449
6461	CVE-2015-4022	High		Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-438
6462	CVE-2015-4021	Medium		The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not verify that the first character of a filename is different from the \0 character, which allows remote attackers to cause a denial of service (integer underflow and memory corruption) via a crafted entry in a tar archive.	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-439
6463	CVE-2015-4017	MEDIUM	High	Salt before 2014.7.6 does not verify certificates when connecting via the aliyun, proxmox, and splunk modules.	salt	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5149
6464	CVE-2015-4004	High		The OZWPAN driver in the Linux kernel through 4.0.5 relies on an untrusted length field during packet parsing, which allows remote attackers to obtain sensitive information from kernel memory or cause a denial of service (out-of-bounds read and system crash) via a crafted packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-451
6465	CVE-2015-4003	High		The oz_usb_handle_ep_data function in drivers/staging/ozwpan/ozusbsvc1.c in the OZWPAN driver in the Linux kernel through 4.0.5 allows remote attackers to cause a denial of service (divide-by-zero error and system crash) via a crafted packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-437
6466	CVE-2015-4002	High		drivers/staging/ozwpan/ozusbsvc1.c in the OZWPAN driver in the Linux kernel through 4.0.5 does not ensure that certain length values are sufficiently large, which allows remote attackers to cause a denial of service (system crash or large loop) or possibly execute arbitrary code via a crafted packet, related to the (1) oz_usb_rx and (2) oz_usb_handle_ep_data functions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-457
6467	CVE-2015-4001	High		Integer signedness error in the oz_hcd_get_desc_cnf function in drivers/staging/ozwpan/ozhcd.c in the OZWPAN driver in the Linux kernel through 4.0.5 allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a crafted packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-442
6468	CVE-2015-4000	Medium	Low	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the Logjam issue.	openssl openssh	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-377

	A	B	C	D	E	F	G	H	I	J	K	L	M
6469	CVE-2015-3991	HIGH	Critical	A flaw was found in the strongSwan payload handling code. This flaw can be triggered by an IKEv1 or IKEv2 message that contains payloads that are only defined for the respective other IKE version. For instance, sending an IKEv1 Main Mode message containing a payload with type 41 (IKEv2 Notify) will crash the daemon or, potentially allow for remote code execution, when a short summary of the contents of the message is logged ("parsed ID_PROT request 0 [...]").	strongswan	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-622
6470	CVE-2015-3903	Medium		libraries/Config.class.php in phpMyAdmin 4.0.x before 4.0.10.10, 4.2.x before 4.2.13.3, 4.3.x before 4.3.13.1, and 4.4.x before 4.4.6.1 disables X.509 certificate verification for GitHub API calls over SSL, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	phpmyadmin	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-391
6471	CVE-2015-3902	Medium		Multiple cross-site request forgery (CSRF) vulnerabilities in the setup process in phpMyAdmin 4.0.x before 4.0.10.10, 4.2.x before 4.2.13.3, 4.3.x before 4.3.13.1, and 4.4.x before 4.4.6.1 allow remote attackers to hijack the authentication of administrators for requests that modify the configuration file.	phpmyadmin	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-388
6472	CVE-2015-3644	Medium		Stunnel 5.00 through 5.13, when using the redirect option, does not redirect client connections to the expected server after the initial connection, which allows remote attackers to bypass authentication.	stunnel	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-359
6473	CVE-2015-3636	MEDIUM		It was found that the Linux kernel's ping socket implementation didn't properly handle socket unhashing during spurious disconnects which could lead to use-after-free flaw.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-401
6474	CVE-2015-3631	Low		Docker Engine before 1.6.1 allows local users to set arbitrary Linux Security Modules (LSM) and docker_t policies via an image that allows volumes to override files in /proc.	docker	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2427
6475	CVE-2015-3630	High		Docker Engine before 1.6.1 uses weak permissions for (1) /proc/asound, (2) /proc/timer_stats, (3) /proc/latency_stats, and (4) /proc/fs, which allows local users to modify the host, obtain sensitive information, and perform protocol downgrade attacks via a crafted image.	docker	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2424
6476	CVE-2015-3629	High		Libcontainer 1.6.0, as used in Docker Engine, allows local users to escape containerization (mount namespace breakout) and write to arbitrary file on the host system via a symlink attack in an image when respawning a container.	libcontainer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2426
6477	CVE-2015-3627	High		Libcontainer and Docker Engine before 1.6.1 opens the file-descriptor passed to the pid-1 process before performing the chroot, which allows local users to gain privileges via a symlink attack in an image.	docker	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2428
6478	CVE-2015-3622	Medium		The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.5 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted certificate.	libtasn1	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-369
6479	CVE-2015-3456	High		The Floppy Disk Controller (FDC) in QEMU, as used in Xen 4.5.x and earlier and KVM, allows local guest users to cause a denial of service (out-of-bounds write and guest crash) or possibly execute arbitrary code via the (1) FD_CMD_READ_ID, (2) FD_CMD_DRIVE_SPECIFICATION_COMMAND, or other unspecified commands, aka VENOM.Though the VENOM vulnerability is also agnostic of the guest operating system, an attacker (or an attacker?? malware) would need to have administrative or root privileges in the guest operating system in order to exploit VENOM	qemu	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-355
6480	CVE-2015-3455	Low		Squid 3.2.x before 3.2.14, 3.3.x before 3.3.14, 3.4.x before 3.4.13, and 3.5.x before 3.5.4, when configured with client-first SSL-bump, does not properly validate the domain or hostname fields of X.509 certificates, which allows man-in-the-middle attackers to spoof SSL servers via a valid certificate.	squid	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-389
6481	CVE-2015-3451	Medium		The _clone function in XML::LibXML before 2.0119 does not properly set the expand_entities option, which allows remote attackers to conduct XML external entity (XXE) attacks via a crafted XML data to the (1) new or (2) load_xml function.CWE-611: Improper Restriction of XML External Entity Reference ('XXE')	libxml-perl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-368
6482	CVE-2015-3420	MEDIUM	Medium	The ssl-proxy-openssl.c function in Dovecot before 2.2.17, when SSLv3 is disabled, allow remote attackers to cause a denial of service (login process crash) via vectors related to handshake failures.	dovecot	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5433
6483	CVE-2015-3418	MEDIUM	High	The ProcPutImage function in dix/dispatch.c in X.Org Server (aka xserver and xorg-server) before 1.16.4 allows attackers to cause a denial of service (divide-by-zero and crash) via a zero-height PutImage request.	xorg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2735
6484	CVE-2015-3417	Medium		Use-after-free vulnerability in the ff_h264_free_tables function in libavcodec/h264.c in FFmpeg before 2.3.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted H.264 data in an MP4 file, as demonstrated by an HTML VIDEO element that references H.264 data.CWE-416: Use After Free	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-313
6485	CVE-2015-3416	High		The sqlite3VXPrintf function in printf.c in SQLite before 3.8.9 does not properly handle precision and width values during floating-point conversions, which allows context-dependent attackers to cause a denial of service (integer overflow and stack-based buffer overflow) or possibly have unspecified other impact via large integers in a crafted printf function call in a SELECT statement.	sqlite	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-332

	A	B	C	D	E	F	G	H	I	J	K	L	M
6486	CVE-2015-3415	High		The sqlite3VdbeExec function in vdbe.c in SQLite before 3.8.9 does not properly implement comparison operators, which allows context-dependent attackers to cause a denial of service (invalid free operation) or possibly have unspecified other impact via a crafted CHECK clause, as demonstrated by CHECK(0&O>O) in a CREATE TABLE statement.	sqlite	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-337
6487	CVE-2015-3414	High		SQLite before 3.8.9 does not properly implement the dequoting of collation-sequence names, which allows context-dependent attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted COLLATE clause, as demonstrated by COLLATE at the end of a SELECT statement.	sqlite	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-335
6488	CVE-2015-3412	Medium	Medium	PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read arbitrary files via crafted input to an application that calls the stream_resolve_include_path function in ext/standard/streamsfuncs.c, as demonstrated by a filename\0.extension attack that bypasses an intended configuration in which client users may read files with only one specific extension.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-716
6489	CVE-2015-3411	Medium	Medium	PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument load method, (2) the xmlwriter_open_uri function, (3) the finfo_file function, or (4) the hash_hmac_file function, as demonstrated by a filename\0.xml attack that bypasses an intended configuration in which client users may read only .xml files.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-737
6490	CVE-2015-3405	MEDIUM	High	A flaw was found in the way the ntp-keygen utility generated MD5 symmetric keys on big-endian systems. This could possibly allow an attacker to guess generated MD5 keys that could then be used to spoof an NTP client or server.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-464
6491	CVE-2015-3395	Medium		The msrle_decode_pal4 function in msrledec.c in Libav before 10.7 and 11.x before 11.4 and FFmpeg before 2.0.7, 2.2.x before 2.2.15, 2.4.x before 2.4.8, 2.5.x before 2.5.6, and 2.6.x before 2.6.2 allows remote attackers to have unspecified impact via a crafted image, related to a pixel pointer, which triggers an out-of-bounds array access.	gst-ffmpeg & libav	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-515
6492	CVE-2015-3339	Medium		Race condition in the prepare_binprm function in fs/exec.c in the Linux kernel before 3.19.6 allows local users to gain privileges by executing a setuid program at a time instant when a chown to root is in progress, and the ownership is changed but the setuid bit is not yet stripped.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-393
6493	CVE-2015-3332	Medium		A certain backport in the TCP Fast Open implementation for the Linux kernel before 3.18 does not properly maintain a count value, which allow local users to cause a denial of service (system crash) via the Fast Open feature, as demonstrated by visiting the chrome://flags/#enable-tcp-fast-open URL when using certain 3.10.x through 3.16.x kernel builds, including longterm-maintenance releases and ckt (aka Canonical Kernel Team) builds.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-390
6494	CVE-2015-3331	High		The __driver_rfc4106_decrypt function in arch/x86/crypto/aesni-intel_glue.c in the Linux kernel before 3.19.3 does not properly determine the memory locations used for encrypted data, which allows context-dependent attackers to cause a denial of service (buffer overflow and system crash) or possibly execute arbitrary code by triggering a crypto API call, as demonstrated by use of a libkcapi test program with an AF_ALG(aead) socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-386
6495	CVE-2015-3330	Medium		The php_handler function in sapi/apache2handler/sapi_apache2.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, when the Apache HTTP Server 2.4.x is used, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via pipelined HTTP requests that result in a deconfigured interpreter.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-448
6496	CVE-2015-3329	High		Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-452
6497	CVE-2015-3310	Medium		Buffer overflow in the rc_mksid function in plugins/radius/util.c in Paul's PPP Package (ppp) 2.4.6 and earlier, when the PID for pppd is greater than 65535, allows remote attackers to cause a denial of service (crash) via a start accounting message to the RADIUS server.	ppp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-336
6498	CVE-2015-3308	High		Double free vulnerability in lib/x509/x509_ext.c in GnuTLS before 3.3.14 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted CRL distribution point.CWE-415: Double Free	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-878
6499	CVE-2015-3307	High		The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-447
6500	CVE-2015-3306	High		The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.	proftpd	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-392

	A	B	C	D	E	F	G	H	I	J	K	L	M
6501	CVE-2015-3291	Low		arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform does not properly determine when nested NMI processing is occurring, which allows local users to cause a denial of service (skipped NMI) by modifying the rsp register, issuing a syscall instruction, and triggering an NMI.	linux	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-206
6502	CVE-2015-3290	High		arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform improperly relies on espfix64 during nested NMI processing, which allows local users to gain privileges by triggering an NMI within a certain instruction window.	linux	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-202
6503	CVE-2015-3289	MEDIUM		OpenStack Glance before 2015.1.1 (kilo) allows remote authenticated users to cause a denial of service (disk consumption) by repeatedly using the import task flow API to create images and then deleting them.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2519
6504	CVE-2015-3288	High	High	mm/memory.c in the Linux kernel before 4.1.4 mishandles anonymous pages, which allows local users to gain privileges or cause a denial of service (page tainting) via a crafted application that triggers writing to page zero.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1833
6505	CVE-2015-3276	Medium		The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyword mode cipher strings, which might cause a weaker than intended cipher to be used and allow remote attackers to have unspecified impact via unknown vectors.	openldap	Unchanged	8.0.0.1	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2210
6506	CVE-2015-3256	Medium		PolicyKit (aka polkit) before 0.113 allows local users to cause a denial of service (memory corruption and polkitd daemon crash) and possibly gain privileges via unspecified vectors, related to javascript rule evaluation.	polkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1329
6507	CVE-2015-3255	Medium		The polkit_backend_action_pool_init function in polkitbackend/polkitbackendactionpool.c in PolicyKit (aka polkit) before 0.113 might allow local users to gain privileges via duplicate action IDs in action descriptions.	polkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1347
6508	CVE-2015-3248	Medium	Medium	openhpi/Makefile.am in OpenHPI before 3.6.0 uses world-writable permissions for /var/lib/openhpi directory, which allows local users, when quotas are not properly setup, to fill the filesystem hosting /var/lib and cause a denial of service (disk consumption).	openhpi	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5533
6509	CVE-2015-3246	High		libuser before 0.56.13-8 and 0.60 before 0.60-7, as used in the userhelper program in the usermode package, directly modifies /etc/passwd, which allows local users to cause a denial of service (inconsistent file state) by causing an error during the modification. NOTE: this issue can be combined with CVE-2015-3245 to gain privileges.	libuser	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-702
6510	CVE-2015-3245	Low		Incomplete blacklist vulnerability in the chfn function in libuser before 0.56.13-8 and 0.60 before 0.60-7, as used in the userhelper program in the usermode package, allows local users to cause a denial of service (/etc/passwd corruption) via a newline character in the GECOS field.	libuser	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-717
6511	CVE-2015-3243	LOW	Medium	rsyslog uses weak permissions for generating log files, which allows local users to obtain sensitive information by reading files in /var/log/cron.	rsyslog	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4854
6512	CVE-2015-3239	Low		Off-by-one error in the dwarf_to_unw_regnum function in include/dwarf_i.h in libunwind 1.1 allows local users to have unspecified impact via invalid dwarf opcodes.	libunwind	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-780
6513	CVE-2015-3238	MEDIUM	Medium	A vulnerability has been discovered in the PAM library (aka Linux-PAM) on Linux/Unix systems. It allows a malicious user to remotely perform harmful actions on a vulnerable system.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-594
6514	CVE-2015-3237	Medium		The smb_request_state function in cURL and libcurl 7.40.0 through 7.42.1 allows remote SMB servers to obtain sensitive information from memory or cause a denial of service (out-of-bounds read and crash) via crafted length and offset values.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-517
6515	CVE-2015-3236	Medium		cURL and libcurl 7.40.0 through 7.42.1 sends the HTTP Basic authentication credentials for a previous connection when reusing a reset (curl_easy_reset) connection handle to send a request to the same host name, which allows remote attackers to obtain sensitive information via unspecified vectors.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-511
6516	CVE-2015-3228	Medium		Integer overflow in the gs_heap_alloc_bytes function in base/gsmalloc.c in Ghostscript 9.15 and earlier allows remote attackers to cause a denial of service (crash) via a crafted Postscript (ps) file, as demonstrated by using the ps2pdf command, which triggers an out-of-bounds read or write.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-705
6517	CVE-2015-3223	Medium	Medium	The ldb_wildcard_compare function in ldb_match.c in ldb before 1.1.24, as used in the AD LDAP server in Samba 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, mishandles certain zero values, which allows remote attackers to cause a denial of service (infinite loop) via crafted packets.	samba	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-123
6518	CVE-2015-3221	Medium		OpenStack Neutron before 2014.2.4 (juno) and 2015.1.x before 2015.1.1 (kilo), when using the IPTables firewall driver, allows remote authenticated users to cause a denial of service (L2 agent crash) by adding an address pair that is rejected by the ipset tool.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2530
6519	CVE-2015-3219	Medium		Cross-site scripting (XSS) vulnerability in the Orchestration/Stack section in OpenStack Dashboard (Horizon) 2014.2 before 2014.2.4 and 2015.1.x before 2015.1.1 allows remote attackers to inject arbitrary web script or HTML via the description parameter in a heat template, which is not properly handled in the help_text attribute in the Field class.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2529

	A	B	C	D	E	F	G	H	I	J	K	L	M
6520	CVE-2015-3218	Low		The authentication_agent_new function in polkitbackend/polkitbackendinteractiveauthority.c in PolicyKit (aka polkit) before 0.113 allows local users to cause a denial of service (NULL pointer dereference and polkitd daemon crash) by calling RegisterAuthenticationAgent with an invalid object path.CWE-476: NULL Pointer Dereference	polkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1338
6521	CVE-2015-3217	MEDIUM	High	PCRE 7.8 and 8.32 through 8.37, and PCRE2 10.10 mishandle group empty matches, which might allow remote attackers to cause a denial of service (stack-based buffer overflow) via a crafted regular expression, as demonstrated by /^(?:(?(1)\.|([^\\\\W_])?)+)+$/.	pcre	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2772
6522	CVE-2015-3216	Medium		Race condition in a certain Red Hat patch to the PRNG lock implementation in the ssleay_rand_bytes function in OpenSSL, as distributed in openssl-1.0.1e-25.el7 in Red Hat Enterprise Linux (RHEL) 7 and other products, allows remote attackers to cause a denial of service (application crash) by establishing many TLS sessions to a multithreaded server, leading to use of a negative value for a certain length field.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-602
6523	CVE-2015-3214	Medium		The pit_ioport_read in i8254.c in the Linux kernel before 2.6.33 and QEMU before 2.3.1 does not distinguish between read lengths and write lengths, which might allow guest OS users to execute arbitrary code on the host OS by triggering use of an invalid index.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-210
6524	CVE-2015-3213	High		The gesture handling code in Clutter before 1.16.2 allows physically proximate attackers to bypass the lock screen via certain (1) mouse or (2) touch gestures.	clutter	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-709
6525	CVE-2015-3212	Medium		Race condition in net/sctp/socket.c in the Linux kernel before 4.1.2 allows local users to cause a denial of service (list corruption and panic) via a rapid series of system calls related to sockets, as demonstrated by setsockopt calls.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-209
6526	CVE-2015-3210	HIGH	Critical	Heap-based buffer overflow in PCRE 8.34 through 8.37 and PCRE2 10.10 allows remote attackers to execute arbitrary code via a crafted regular expression, as demonstrated by /^(?P=B)((?P=B)(?J:(?P<B>c)(?P<B>a(?P=B)))>WGXCREDITS)/, a different vulnerability than CVE-2015-8384.	pcre	Unchanged	8.0.0.13	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2710
6527	CVE-2015-3209	High		Heap-based buffer overflow in the PCNET controller in QEMU allows remote attackers to execute arbitrary code by sending a packet with TXSTATUS_STARTPACKET set and then a crafted packet with TXSTATUS_DEVICEOWNS set.	qemu	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-513
6528	CVE-2015-3202	LOW		A vulnerability has been discovered in the FUSE subsystem on Linux. It allows a malicious person having an unprivileged account on a vulnerable system to take the full control of this system.	fuse	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-380
6529	CVE-2015-3200	Medium	High	mod_auth in lighttpd before 1.4.36 allows remote attackers to inject arbitrary log entries via a basic HTTP authentication string without a colon character, as demonstrated by a string containing a NULL and new line character.	lighttpd	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-440
6530	CVE-2015-3197	MEDIUM	Medium	an issue where a connecting client can force an SSL handshake to complete via SSLv2, even if allSSLv2 ciphers are disabled. It is important to note that simply disabling the SSLv2 ciphers on your OpenSSL server will not mitigate this issue. In order to prevent an SSLv2 connection, support for the actual protocol must be disabled as well. In other words, even if the server configuration only allows strong ciphers (such as AES-GCM) that are not part of SSLv2, it is possible for an attacker to "slip through" these disabled ciphers and complete a handshake usingSSLv2. SSLv2 is a weak and broken protocol and should not be used. If that's not possible -- and really, the only reason is having to support very old clients	openssl	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-229
6531	CVE-2015-3196	Medium		ssl/s3_clnt.c in OpenSSL 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1p, and 1.0.2 before 1.0.2d, when used for a multi-threaded client, writes the PSK identity hint to an incorrect data structure, which allows remote servers to cause a denial of service (race condition and double free) via a crafted ServerKeyExchange message.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2223
6532	CVE-2015-3195	Medium	Medium	The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.	openssl	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2201
6533	CVE-2015-3194	Medium	High	crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.CWE-476: NULL Pointer Dereference	openssl	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2221
6534	CVE-2015-3193	Medium		The Montgomery squaring implementation in crypto/bn/asm/x86_64-mont5.pl in OpenSSL 1.0.2 before 1.0.2e on the x86_64 platform, as used by the BN_mod_exp function, mishandles carry propagation and produces incorrect output, which makes it easier for remote attackers to obtain sensitive private-key information via an attack against use of a (1) Diffie-Hellman (DH) or (2) Diffie-Hellman Ephemeral (DHE) ciphersuite.	openssl	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2207

	A	B	C	D	E	F	G	H	I	J	K	L	M
6535	CVE-2015-3187	Medium		The svn_repos_trace_node_locations function in Apache Subversion before 1.7.21 and 1.8.x before 1.8.14, when path-based authorization is used, allows remote authenticated users to obtain sensitive path information by reading the history of a node that has been moved from a hidden path.	subversion	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-713
6536	CVE-2015-3185	Medium		The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.	apache	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-658
6537	CVE-2015-3184	Medium		mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.	subversion	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-721
6538	CVE-2015-3183	Medium		The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.	apache	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-651
6539	CVE-2015-3182	Medium	Medium	epan/dissectors/packet-dec-dnart.c in the DECnet NSP/RT dissector in Wireshark 1.10.12 through 1.10.14 mishandles a certain strdup return value, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-116
6540	CVE-2015-3167	Medium		pgcrypto functions usually reported "Wrong key or corrupt data" upon decrypting with an incorrect key, but several other messages were possible when the errant decryption output resembled an OpenPGP packet header. Error message variance in other systems has enabled cryptologic attacks; see RFC 4880 section "14. Security Considerations". Whether these pgcrypto behaviors are likewise exploitable is unknown.	postgresql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-419
6541	CVE-2015-3166	Medium		The server regularly ignores the return value of certain standard library functions, such as sprintf() and putenv(), which can fail under memory exhaustion. This could, in principle, have a variety of security-relevant effects. For example, an unnoticed sprintf() error could permit disclosure of prior buffer contents. A particular putenv() failure could cause GSSAPI authentication to consult the wrong keytab file. Reducing such exploits to practice is expected to be impossible in most configurations, given the requirement for such an intricate coincidence of system state.	postgresql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-418
6542	CVE-2015-3165	Medium		Double free vulnerability in PostgreSQL before 9.0.20, 9.1.x before 9.1.16, 9.2.x before 9.2.11, 9.3.x before 9.3.7, and 9.4.x before 9.4.2 allows remote attackers to cause a denial of service (crash) by closing an SSL session at a time when the authentication timeout will expire during the session shutdown sequence.CWE-415: Double Free	postgresql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-395
6543	CVE-2015-3153	MEDIUM		The default configuration for cURL and libcurl before 7.42.1 sends custom HTTP headers to both the proxy and destination server, which might allow remote proxy servers to obtain sensitive information by reading the header contents.	curl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-314
6544	CVE-2015-3152	Medium	Medium	Oracle MySQL before 5.7.3, Oracle MySQL Connector/C (aka libmysqlclient) before 6.1.3, and MariaDB before 5.5.44 use the --ssl option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, aka a BACKRONYM attack.	mysql	Unchanged	8.0.0.6	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-720
6545	CVE-2015-3149	LOW	Medium	The Hotspot component in OpenJDK8 as packaged in Red Hat Enterprise Linux 6 and 7 allows local users to write to arbitrary files via a symlink attack.	jdk&jre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-7272
6546	CVE-2015-3148	Medium		cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use authenticated Negotiate connections, which allows remote attackers to connect as other users via a request.	curl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-338
6547	CVE-2015-3146	Medium	High	The (1) SSH_MSG_NEWKEYS and (2) SSH_MSG_KEXDH_REPLY packet handlers in package_cb.c in libssh before 0.6.5 do not properly validate state, which allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted SSH packet.CWE-476: NULL Pointer Dereference	libssh	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-515
6548	CVE-2015-3145	High		The sanitize_cookie_path function in cURL and libcurl 7.31.0 through 7.41.0 does not properly calculate an index, which allows remote attackers to cause a denial of service (out-of-bounds write and crash) or possibly have other unspecified impact via a cookie path containing only a double-quote character.	curl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-307
6549	CVE-2015-3144	High		The fix_hostname function in cURL and libcurl 7.37.0 through 7.41.0 does not properly calculate an index, which allows remote attackers to cause a denial of service (out-of-bounds read or write and crash) or possibly have other unspecified impact via a zero-length host name, as demonstrated by http://:80 and :80.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-330
6550	CVE-2015-3143	Medium		cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request, a similar issue to CVE-2014-0015.	curl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-342
6551	CVE-2015-3138	Medium	High	print-wb.c in tcpdump before 4.7.4 allows remote attackers to cause a denial of service (segmentation fault and process crash).	tcpdump	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5578

	A	B	C	D	E	F	G	H	I	J	K	L	M
6552	CVE-2015-2925	Medium		The prepend_path function in fs/dcache.c in the Linux kernel before 4.2.4 does not properly handle rename actions inside a bind mount, which allows local users to bypass an intended container protection mechanism by renaming a directory, related to a double-chroot attack.	linux	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1911
6553	CVE-2015-2922	LOW		Linux kernel built with the IPv6 networking support(CONFIG_IPV6) is vulnerable to setting its 'hop_limit' too low, via the neighbour discovery protocol. It could result in thwarting the IPv6 functionality.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-265
6554	CVE-2015-2830	Low		arch/x86/kernel/entry_64.S in the Linux kernel before 3.19.2 does not prevent the TS_COMPAT flag from reaching a user-mode task, which might allow local users to bypass the seccomp or audit protection mechanism via a crafted application that uses the (1) fork or (2) close system call, as demonstrated by an attack against seccomp before 3.16.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-385
6555	CVE-2015-2808	Medium		The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the Bar Mitzvah issue.	openssl	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN8-292
6556	CVE-2015-2806	High		Stack-based buffer overflow in asn1_der_decoding in libtasn1 before 4.4 allows remote attackers to have unspecified impact via unknown vectors.	libtasn1	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-268
6557	CVE-2015-2787	High		Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages use of the unset function within an __wakeup function, a related issue to CVE-2015-0231.CWE-416: Use After Free	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-286
6558	CVE-2015-2783	Medium		ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read and application crash) via a crafted length value in conjunction with crafted serialized data in a phar archive, related to the phar_parse_metadata and phar_parse_pharfile functions.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-455
6559	CVE-2015-2756	Medium		QEMU, as used in Xen 3.3.x through 4.5.x, does not properly restrict access to PCI command registers, which might allow local HVM guest users to cause a denial of service (non-maskable interrupt and host crash) by disabling the (1) memory or (2) I/O decoding for a PCI Express device and then accessing the device, which triggers an Unsupported Request (UR) response.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-289
6560	CVE-2015-2730	Medium		Mozilla Network Security Services (NSS) before 3.19.1, as used in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and other products, does not properly perform Elliptical Curve Cryptography (ECC) multiplications, which makes it easier for remote attackers to spoof ECDSA signatures via unspecified vectors.	nss	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-600
6561	CVE-2015-2721	Medium		Mozilla Network Security Services (NSS) before 3.19, as used in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, Thunderbird before 38.1, and other products, does not properly determine state transitions for the TLS state machine, which allows man-in-the-middle attackers to defeat cryptographic protection mechanisms by blocking messages, as demonstrated by removing a forward-secrecy property by blocking a ServerKeyExchange message, aka a SMACK SKIP-TLS issue.	nss	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-598
6562	CVE-2015-2716	High		Buffer overflow in the XML parser in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderbird before 31.7 allows remote attackers to execute arbitrary code by providing a large amount of compressed XML data.	expat	Unchanged	8.0.0.7	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1171
6563	CVE-2015-2698	High		The iakerb_gss_export_sec_context function in lib/gssapi/krb5/iakerb.c in MIT Kerberos 5 (aka krb5) 1.14 pre-release 2015-09-14 improperly accesses a certain pointer, which allows remote authenticated users to cause a denial of service (memory corruption) or possibly have unspecified other impact by interacting with an application that calls the gss_export_sec_context function. NOTE: this vulnerability exists because of an incorrect fix for CVE-2015-2696.	krb5	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1910
6564	CVE-2015-2697	Medium		The build_principal_va function in lib/krb5/krb/bld_princ.c in MIT Kerberos 5 (aka krb5) before 1.14 allows remote authenticated users to cause a denial of service (out-of-bounds read and KDC crash) via an initial \0' character in a long realm field within a TGS request.	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1574
6565	CVE-2015-2696	High		lib/gssapi/krb5/iakerb.c in MIT Kerberos 5 (aka krb5) before 1.14 relies on an inappropriate context handle, which allows remote attackers to cause a denial of service (incorrect pointer read and process crash) via a crafted IAKERB packet that is mishandled during a gss_inquire_context call.	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1579
6566	CVE-2015-2695	High		lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) before 1.14 relies on an inappropriate context handle, which allows remote attackers to cause a denial of service (incorrect pointer read and process crash) via a crafted SPNEGO packet that is mishandled during a gss_inquire_context call.	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1578

	A	B	C	D	E	F	G	H	I	J	K	L	M
6567	CVE-2015-2694	Medium		The kdcpreauth modules in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.2 do not properly track whether a client's request has been validated, which allows remote attackers to bypass an intended preauthentication requirement by providing (1) zero bytes of data or (2) an arbitrary realm name, related to plugins/preauth/otp/main.c and plugins/preauth/pkinit/pkinit_srv.c.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-398
6568	CVE-2015-2686	High	High	net/socket.c in the Linux kernel 3.19 before 3.19.3 does not validate certain range data for (1) sendto and (2) recvfrom system calls, which allows local users to gain privileges by leveraging a subsystem that uses the copy_from_iter function in the iov_iter interface, as demonstrated by the Bluetooth subsystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-627
6569	CVE-2015-2672	Medium	Medium	The xsave/xrstor implementation in arch/x86/include/asm/xsave.h in the Linux kernel before 3.19.2 creates certain .altinstr_replacement pointers and consequently does not provide any protection against instruction faulting, which allows local users to cause a denial of service (panic) by triggering a fault, as demonstrated by an unaligned memory operand or a non-canonical address memory operand.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-569
6570	CVE-2015-2666	Medium		Stack-based buffer overflow in the get_matching_model_microcode function in arch/x86/kernel/cpu/microcode/intel_early.c in the Linux kernel before 4.0 allows context-dependent attackers to gain privileges by constructing a crafted microcode header and leveraging root privileges for write access to the initrd.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-394
6571	CVE-2015-2661	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows local users to affect availability via unknown vectors related to Client.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-652
6572	CVE-2015-2648	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-660
6573	CVE-2015-2643	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-656
6574	CVE-2015-2641	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-654
6575	CVE-2015-2639	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server : Security : Firewall.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-648
6576	CVE-2015-2620	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.23 and earlier allows remote authenticated users to affect confidentiality via unknown vectors related to Server : Security : Privileges.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-665
6577	CVE-2015-2617	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-655
6578	CVE-2015-2611	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-646
6579	CVE-2015-2582	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to GIS.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-668
6580	CVE-2015-2576	Low		Unspecified vulnerability in the MySQL Utilities component in Oracle MySQL 1.5.1 and earlier, when running on Windows, allows local users to affect integrity via unknown vectors related to Installation.Per Oracle: This vulnerability is only applicable on Windows operating system (http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html)	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-321
6581	CVE-2015-2575	Medium		Unspecified vulnerability in the MySQL Connectors component in Oracle MySQL 5.1.34 and earlier allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Connector/J.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-324
6582	CVE-2015-2573	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier, allows remote authenticated users to affect availability via vectors related to DDL.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-317
6583	CVE-2015-2571	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-331
6584	CVE-2015-2568	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier, allows remote attackers to affect availability via unknown vectors related to Server : Security : Privileges.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-340
6585	CVE-2015-2567	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-309
6586	CVE-2015-2566	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-334
6587	CVE-2015-2348	Medium		The move_uploaded_file implementation in ext/standard/basic_functions.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 truncates a pathname upon encountering a \x00 character, which allows remote attackers to bypass intended extension restrictions and create files with unexpected names via a crafted second argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-273

	A	B	C	D	E	F	G	H	I	J	K	L	M
6588	CVE-2015-2331	High		Integer overflow in the _zip_cdir_new function in zip_dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-285
6589	CVE-2015-2330	MEDIUM	High	Late TLS certificate verification in WebKitGTK+ prior to 2.6.6 allows remote attackers to view a secure HTTP request, including, for example, secure cookies.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3541
6590	CVE-2015-2328	High		PCRE before 8.36 mishandles the /((?(R)a|(?1))+/ pattern and related patterns with certain recursion, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2198
6591	CVE-2015-2327	High		PCRE before 8.36 mishandles the /(((a\ 2)|(a*)\g<-1>))*/ pattern and related patterns with certain internal recursive back references, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted regular expression, as demonstrated by a JavaScript RegExp object encountered by Konqueror.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2214
6592	CVE-2015-2305	Medium		Integer overflow in the regcomp implementation in the Henry Spencer BSD regex library (aka rxspencer) alpha3.8.g5 on 32-bit platforms, as used in NetBSD through 6.1.5 and other products, might allow context-dependent attackers to execute arbitrary code via a large regular expression that leads to a heap-based buffer overflow.	mysql & php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-295
6593	CVE-2015-2304	Medium		Absolute path traversal vulnerability in bsdcpio in libarchive 3.1.2 and earlier allows remote attackers to write to arbitrary files via a full pathname in an archive.	libarchive	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-248
6594	CVE-2015-2301	High		Use-after-free vulnerability in the phar_rename_archive function in phar_object.c in PHP before 5.5.22 and 5.6.x before 5.6.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted renaming of a Phar archive to the name of an existing file.CWE-416: Use After Free	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-270
6595	CVE-2015-2214	Medium		NetCat 5.01 and earlier allows remote attackers to obtain the installation path via the redirect_url parameter to netshop/post.php.	netcat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-221
6596	CVE-2015-2206	Medium		libraries/select_lang.lib.php in phpMyAdmin 4.0.x before 4.0.10.9, 4.2.x before 4.2.13.2, and 4.3.x before 4.3.11.1 includes invalid language values in unknown-language error responses that contain a CSRF token and may be sent with HTTP compression, which makes it easier for remote attackers to conduct a BREACH attack and determine this token via a series of crafted requests.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-218
6597	CVE-2015-2155	High		The force printer in tcpdump before 4.7.2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors.	tcpdump	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-255
6598	CVE-2015-2154	Medium		The osi_print_cksum function in print-isoclns.c in the ethernet printer in tcpdump before 4.7.2 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted (1) length, (2) offset, or (3) base pointer checksum value.	tcpdump	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-243
6599	CVE-2015-2153	Medium		The rpki_rtr_pdu_print function in print-rpki-rtr.c in the TCP printer in tcpdump before 4.7.2 allows remote attackers to cause a denial of service (out-of-bounds read or write and crash) via a crafted header length in an RPKI-RTR Protocol Data Unit (PDU).	tcpdump	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-259
6600	CVE-2015-2150	Medium		Xen 3.3.x through 4.5.x does not properly restrict access to PCI command registers, which might allow local guest users to cause a denial of service (non-maskable interrupt and host crash) by disabling the (1) memory or (2) I/O decoding for a PCI Express device and then accessing the device, which triggers an Unsupported Request (UR) response.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4206
6601	CVE-2015-2059	High		The stringprep_utf8_to_ucs4 function in libin before 1.31, as used in jabberd2, allows context-dependent attackers to read system memory and possibly have other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read.	libidn	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-712
6602	CVE-2015-2042	Medium		net/rds/sysctl.c in the Linux kernel before 3.19 uses an incorrect data type in a sysctl table, which allows local users to obtain potentially sensitive information from kernel memory or possibly have unspecified other impact by accessing a sysctl entry.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-306
6603	CVE-2015-2041	Medium		net/llc/sysctl_net_llc.c in the Linux kernel before 3.19 uses an incorrect data type in a sysctl table, which allows local users to obtain potentially sensitive information from kernel memory or possibly have unspecified other impact by accessing a sysctl entry.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-318
6604	CVE-2015-1881	MEDIUM		OpenStack Image Registry and Delivery Service (Glance) 2014.2 through 2014.2.2 does not properly remove images, which allows remote authenticated users to cause a denial of service (disk consumption) by creating a large number of images using the task v2 API and then deleting them, a different vulnerability than CVE-2014-9684.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2322
6605	CVE-2015-1872	Medium		The ff_mjpeg_decode_sof function in libavcodec/mjpegdec.c in FFmpeg before 2.5.4 does not validate the number of components in a JPEG-LS Start Of Frame segment, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Motion JPEG data.	gst-ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-669

	A	B	C	D	E	F	G	H	I	J	K	L	M
6606	CVE-2015-1867	High		Pacemaker before 1.1.13 does not properly evaluate added nodes, which allows remote read-only users to gain privileges via an acl command.	pacemaker	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-708
6607	CVE-2015-1865	LOW	Medium	fts.c in coreutils 8.4 allows local users to delete arbitrary files.	coreutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5431
6608	CVE-2015-1863	Medium		Heap-based buffer overflow in wpa_supplicant 1.0 through 2.4 allows remote attackers to cause a denial of service (crash), read memory, or possibly execute arbitrary code via crafted SSID information in a management frame when creating or updating P2P entries.	wpa_supplicant	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-328
6609	CVE-2015-1860	Medium		Multiple buffer overflows in the QtBase module in Qt before 4.8.7 and 5.x before 5.4.2 allow remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted GIF image.	qt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-364
6610	CVE-2015-1859	Medium		Multiple buffer overflows in the QtBase module in Qt before 4.8.7 and 5.x before 5.4.2 allow remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted ICO image.	qt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-362
6611	CVE-2015-1858	Medium		Multiple buffer overflows in the QtBase module in Qt before 4.8.7 and 5.x before 5.4.2 allow remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted BMP image.	qt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-365
6612	CVE-2015-1851	Medium		OpenStack Cinder before 2014.1.5 (icehouse), 2014.2.x before 2014.2.4 (juno), and 2015.1.x before 2015.1.1 (kilo) allows remote authenticated users to read arbitrary files via a crafted qcow2 signature in an image to the upload-to-image command.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2479
6613	CVE-2015-1843	Medium		The Red Hat docker package before 1.5.0-28, when using the --add-registry option, falls back to HTTP when the HTTPS connection to the registry fails, which allows man-in-the-middle attackers to conduct downgrade attacks and obtain authentication and image data by leveraging a network position between the client and the registry to block HTTPS traffic. NOTE: this vulnerability exists because of a CVE-2014-5277 regression.	docker	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2387
6614	CVE-2015-1828	MEDIUM	Medium	The Ruby http gem before 0.7.3 does not verify hostnames in SSL connections, which might allow remote attackers to obtain sensitive information via a man-in-the-middle-attack.	ruby	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5586
6615	CVE-2015-1820	HIGH	Critical	REST client for Ruby (aka rest-client) before 1.8.0 allows remote attackers to conduct session fixation attacks or obtain sensitive cookie information by leveraging passage of cookies set in a response to a redirect.	rest-client	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5032
6616	CVE-2015-1819	MEDIUM		CVE-2015-1819 Enforce the reader to run in constant memory	libxml2	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-287
6617	CVE-2015-1817	HIGH	Critical	Stack-based buffer overflow in the inet_pton function in network/inet_pton.c in musl libc 0.9.15 through 1.0.4, and 1.1.0 through 1.1.7 allows attackers to have unspecified impact via unknown vectors.	musl	Unchanged	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5166
6618	CVE-2015-1805	HIGH		A flaw was found in the way pipe_iov_copy_from_user() and Pipe_iov_copy_to_user() functions handled iovecs remaining len accounting on failed atomic access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-407
6619	CVE-2015-1804	High		The bdfReadCharacters function in bitmap/bdfread.c in X.Org libXfont before 1.4.9 and 1.5.x before 1.5.1 does not properly perform type conversion for metrics values, which allows remote authenticated users to cause a denial of service (out-of-bounds memory access) and possibly execute arbitrary code via a crafted BDF font file.	libxfont	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-246
6620	CVE-2015-1803	High		The bdfReadCharacters function in bitmap/bdfread.c in X.Org libXfont before 1.4.9 and 1.5.x before 1.5.1 does not properly handle character bitmaps it cannot read, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) and possibly execute arbitrary code via a crafted BDF font file.CWE-476: NULL Pointer Dereference	libxfont	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-236
6621	CVE-2015-1802	High		The bdfReadProperties function in bitmap/bdfread.c in X.Org libXfont before 1.4.9 and 1.5.x before 1.5.1 allows remote authenticated users to cause a denial of service (out-of-bounds write and crash) or possibly execute arbitrary code via a (1) negative or (2) large property count in a BDF font file.	libxfont	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-251
6622	CVE-2015-1799	Medium		The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 3.x and 4.x before 4.2.8p2 performs state-variable updates upon receiving certain invalid packets, which makes it easier for man-in-the-middle attackers to cause a denial of service (synchronization loss) by spoofing the source IP address of a peer.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-262
6623	CVE-2015-1798	Low		The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p2 requires a correct MAC only if the MAC field has a nonzero length, which makes it easier for man-in-the-middle attackers to spoof packets by omitting the MAC.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-261
6624	CVE-2015-1794	Medium		The ssl3_get_key_exchange function in ssl/s3_clnt.c in OpenSSL 1.0.2 before 1.0.2e allows remote servers to cause a denial of service (segmentation fault) via a zero p value in an anonymous Diffie-Hellman (DH) ServerKeyExchange message.	openssl	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2196
6625	CVE-2015-1793	Medium	Medium	The X509_verify_cert function in crypto/x509/x509_vfy.c in OpenSSL 1.0.1n, 1.0.1o, 1.0.2b, and 1.0.2c does not properly process X.509 Basic Constraints cA values during identification of alternative certificate chains, which allows remote attackers to spoof a Certification Authority role and trigger unintended certificate verifications via a valid leaf certificate.	openssl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-599

	A	B	C	D	E	F	G	H	I	J	K	L	M
6626	CVE-2015-1792	MEDIUM		The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.	openssl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-456
6627	CVE-2015-1791	MEDIUM		Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.	openssl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-436
6628	CVE-2015-1790	MEDIUM		The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.	openssl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-458
6629	CVE-2015-1789	MEDIUM	High	The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.	openssl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-444
6630	CVE-2015-1788	MEDIUM		The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.	openssl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-454
6631	CVE-2015-1787	Low		The ssl3_get_client_key_exchange function in s3_srvr.c in OpenSSL 1.0.2 before 1.0.2a, when client authentication and an ephemeral Diffie-Hellman ciphersuite are enabled, allows remote attackers to cause a denial of service (daemon crash) via a ClientKeyExchange message with a length of zero.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-253
6632	CVE-2015-1782	Medium		The kex_agree_methods function in libssh2 before 1.5.0 allows remote servers to cause a denial of service (crash) or have other unspecified impact via crafted length values in an SSH_MSG_KEXINIT packet.	libssh2	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-212
6633	CVE-2015-1781	MEDIUM		Arjun Shankar of Red Hat discovered that gethostbyname_r and related functions compute the size of an input buffer incorrectly if the passed-in buffer is misaligned. This results in a buffer overflow.	glibc	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-357
6634	CVE-2015-1779	HIGH	High	The VNC websocket frame decoder in QEMU allows remote attackers to cause a denial of service (memory and CPU consumption) via a large (1) websocket payload or (2) HTTP headers section.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-137
6635	CVE-2015-1593	Medium		The stack randomization feature in the Linux kernel before 3.19.1 on 64-bit platforms uses incorrect data types for the results of bitwise left-shift operations, which makes it easier for attackers to bypass the ASLR protection mechanism by predicting the address of the top of the stack, related to the randomize_stack_top function in fs/binfmt_elf.c and the stack_maxrandom_size function in arch/x86/mm/mmap.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-223
6636	CVE-2015-1573	Medium	Medium	The nft_flush_table function in net/netfilter/nf_tables_api.c in the Linux kernel before 3.18.5 mishandles the interaction between cross-chain jumps and ruleset flushes, which allows local users to cause a denial of service (panic) by leveraging the CAP_NET_ADMIN capability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-618
6637	CVE-2015-1572	MEDIUM		Heap-based buffer overflow in closefs.c in the libext2fs library in e2fsprogs before 1.42.12 allows local users to execute arbitrary code by causing a crafted block group descriptor to be marked as dirty. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-0247.	e2fsprogs	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-219
6638	CVE-2015-1563	Low		The ARM GIC distributor virtualization in Xen 4.4.x and 4.5.x allows local guests to cause a denial of service by causing a large number messages to be logged.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2321
6639	CVE-2015-1547	Medium	Medium	The NeXTDecode function in tif_next.c in LibTIFF allows remote attackers to cause a denial of service (uninitialized memory access) via a crafted TIFF image, as demonstrated by libtiff5.tif.	libtiff	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-468
6640	CVE-2015-1546	Medium		Double free vulnerability in the get_vrFilter function in servers/slapd/filter.c in OpenLDAP 2.4.40 allows remote attackers to cause a denial of service (crash) via a crafted search query with a matched values control.CWE - CWE-415: Double Free	openldap	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-171
6641	CVE-2015-1545	Medium		The deref_parseCtrl function in servers/slapd/overlays/deref.c in OpenLDAP 2.4.13 through 2.4.40 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via an empty attribute list in a deref control in a search request.CWE-476: NULL Pointer Dereference	openldap	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-189

	A	B	C	D	E	F	G	H	I	J	K	L	M
6642	CVE-2015-1473	Medium		The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not properly consider data-type size during a risk-management decision for use of the alloca function, which might allow context-dependent attackers to cause a denial of service (segmentation violation) or overwrite memory locations beyond the stack boundary via a long line containing wide characters that are improperly handled in a wscanf call.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-293
6643	CVE-2015-1472	High		The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not properly consider data-type size during memory allocation, which allows context-dependent attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a long line containing wide characters that are improperly handled in a wscanf call.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-269
6644	CVE-2015-1465	High		The IPv4 implementation in the Linux kernel before 3.18.8 does not properly consider the length of the Read-Copy Update (RCU) grace period for redirecting lookups in the absence of caching, which allows remote attackers to cause a denial of service (memory consumption or system crash) via a flood of packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-271
6645	CVE-2015-1421	High		Use-after-free vulnerability in the sctp_assoc_update function in net/sctp/associola.c in the Linux kernel before 3.18.8 allows remote attackers to cause a denial of service (slab corruption and panic) or possibly have unspecified other impact by triggering an INIT collision that leads to improper handling of shared-key data.CWE-416: Use After Free	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-247
6646	CVE-2015-1420	Low		Race condition in the handle_to_path function in fs/fhandle.c in the Linux kernel through 3.19.1 allows local users to bypass intended size restrictions and trigger read operations on additional memory locations by changing the handle_bytes value of a file handle during the execution of this function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-254
6647	CVE-2015-1419	Medium		Unspecified vulnerability in vsftp 3.0.2 and earlier allows remote attackers to bypass access restrictions via unknown vectors, related to deny_file parsing.	vsftpd	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-122
6648	CVE-2015-1395	HIGH	High	Directory traversal vulnerability in GNU patch versions which support Git-style patching before 2.7.3 allows remote attackers to write to arbitrary files with the permissions of the target user via a .. (dot dot) in a diff file name.	patch	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5162
6649	CVE-2015-1379	MEDIUM	High	The signal handler implementations in socat before 1.7.3.0 and 2.0.0-b8 allow remote attackers to cause a denial of service (process freeze or crash).	socat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4382
6650	CVE-2015-1377	Medium		The Read Mail module in Webmin 1.720 allows local users to read arbitrary files via a symlink attack on an unspecified file.	webmin	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-202
6651	CVE-2015-1353	High		Multiple integer overflows in the calendar extension in PHP through 5.6.7 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted year value to (1) the GregorianToSdn function in gregor.c or (2) the JulianToSdn function in julian.c, as demonstrated by a crafted third argument to the gregoriantojd or juliantojd function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-278
6652	CVE-2015-1352	Medium		The build_tablename function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP through 5.6.7 does not validate token extraction for table names, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name.CWE-476: NULL Pointer Dereference	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-280
6653	CVE-2015-1351	High		Use-after-free vulnerability in the _zend_shared_memdup function in zend_shared_alloc.c in the OPcache extension in PHP through 5.6.7 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.CWE-416: Use After Free	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-275
6654	CVE-2015-1350	Low	Medium	The VFS subsystem in the Linux kernel 3.x provides an incomplete set of requirements for setattr operations that underspecifies removing extended privilege attributes, which allows local users to cause a denial of service (capability stripping) via a failed invocation of a system call, as demonstrated by using chown to remove a capability from the ping or Wireshark dumpcap program.	linux	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-624
6655	CVE-2015-1349	Medium		named in ISC BIND 9.7.0 through 9.9.6 before 9.9.6-P2 and 9.10.x before 9.10.1-P2, when DNSSEC validation and the managed-keys feature are enabled, allows remote attackers to cause a denial of service (assertion failure and daemon exit, or daemon crash) by triggering an incorrect trust-anchor management scenario in which no key is ready for use.	bind	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-176
6656	CVE-2015-1345	Low		The bmexec_trans function in kwset.c in grep 2.19 through 2.21 allows local users to cause a denial of service (out-of-bounds heap read and crash) via crafted input when using the -F option.	grep	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-192
6657	CVE-2015-1339	Medium	Medium	Memory leak in the cuse_channel_release function in fs/fuse/cuse.c in the Linux kernel before 4.4 allows local users to cause a denial of service (memory consumption) or possibly have unspecified other impact by opening /dev/cuse many times.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-598
6658	CVE-2015-1335	High		lxc-start in lxc before 1.0.8 and 1.1.x before 1.1.4 allows local container administrators to escape AppArmor confinement via a symlink attack on a (1) mount target or (2) bind mount source.	lxc	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1083

	A	B	C	D	E	F	G	H	I	J	K	L	M
6659	CVE-2015-1334	Medium		attach.c in LXC 1.1.2 and earlier uses the proc filesystem in a container, which allows local container users to escape AppArmor or SELinux confinement by mounting a poc filesystem with a crafted (1) AppArmor profile or (2) SELinux label.	lxc	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-718
6660	CVE-2015-1333	Medium		Memory leak in the __key_link_end function in security/keys/keyring.c in the Linux kernel before 4.1.4 allows local users to cause a denial of service (memory consumption) via many add_key system calls that refer to existing keys.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-212
6661	CVE-2015-1331	Medium		lxclock.c in LXC 1.1.2 and earlier allows local users to create arbitrary files via a symlink attack on /run/lock/lxc/*.	lxc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-704
6662	CVE-2015-1326	High	HIGH	python-dbusmock before version 0.15.1 AddTemplate() D-Bus method call or DBusTestCase.spawn_server_template() method could be tricked into executing malicious code if an attacker supplies a .pyc file.	python-dbusmock	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-3930
6663	CVE-2015-1315	High		Buffer overflow in the charset_to_intern function in unix/unix.c in Info-Zip UnZip 6.10b allows remote attackers to execute arbitrary code via a crafted string, as demonstrated by converting a string from CP866 to UTF-8.	unzip	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-183
6664	CVE-2015-1283	Medium		Multiple integer overflows in the XML_GetBuffer function in Expat through 2.1.0, as used in Google Chrome before 44.0.2403.89 and other products, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted XML data, a related issue to CVE-2015-2716.	expat	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2281
6665	CVE-2015-1239	MEDIUM	Medium	Double free vulnerability in the j2k_read_ppm_v3 function in OpenJPEG before r2997, as used in PDFium in Google Chrome, allows remote attackers to cause a denial of service (process crash) via a crafted PDF.	openjpeg	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5677
6666	CVE-2015-1208			Integer underflow in the mov_read_default function in libavformat/mov.c in FFmpeg before 2.4.6 allows remote attackers to obtain sensitive information from heap and/or stack memory via a crafted MP4 file.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3100
6667	CVE-2015-1197	Low		cpio 2.11, when using the --no-absolute-filenames option, allows local users to write to arbitrary files via a symlink attack on a file in an archive.CWE-61: UNIX Symbolic Link (Symlink) Following	cpio	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-167
6668	CVE-2015-1196	Medium		GNU patch 2.7.1 allows remote attackers to write to arbitrary files via a symlink attack in a patch file.	patch	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-118
6669	CVE-2015-1194	Medium		pax 1:20140703 allows remote attackers to write to arbitrary files via a symlink attack in an archive.	pax	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-119
6670	CVE-2015-1193	Medium		Multiple directory traversal vulnerabilities in pax 1:20140703 allow remote attackers to write to arbitrary files via a (1) full pathname or (2) .. (dot dot) in an archive.	pax	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-137
6671	CVE-2015-1191	Medium		Multiple directory traversal vulnerabilities in pigz 2.3.1 allow remote attackers to write to arbitrary files via a (1) full pathname or (2) .. (dot dot) in an archive.	pigz	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-131
6672	CVE-2015-1182	High		The asn1_get_sequence_of function in library/asn1parse.c in PolarSSL 1.0 through 1.2.12 and 1.3.x through 1.3.9 does not properly initialize a pointer in the asn1_sequence linked list, which allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted ASN.1 sequence in a certificate.CWE-824: Access of Uninitialized Pointer	polarssl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-136
6673	CVE-2015-1159	MEDIUM		A cross-site scripting bug in the CUPS templating engine allows this bug to be exploited when a user browses the web. This XSS is reachable in the default configuration for Linux instances of CUPS, and allows an attacker to bypass default configuration settings that bind the CUPS scheduler to the 'localhost' or loopback interface.	cups	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-429
6674	CVE-2015-1158	HIGH		Cupsd uses reference-counted strings with global scope. When parsing a print job request, cupsd over-decrements the reference count for a string from the request. As a result, an attacker can prematurely free an arbitrary string of global scope. They can use this to dismantle ACLs protecting privileged operations, and upload a replacement configuration file, and subsequently run arbitrary code on a target machine.	cups	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-428
6675	CVE-2015-0973	High		Buffer overflow in the png_read_IDAT_data function in pngrutil.c in libpng before 1.5.21 and 1.6.x before 1.6.16 allows context-dependent attackers to execute arbitrary code via IDAT data with a large width, a different vulnerability than CVE-2014-9495.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-121
6676	CVE-2015-0928	Medium	High	libhtp 0.5.15 allows remote attackers to cause a denial of service (NULL pointer dereference).	libhtp	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5362
6677	CVE-2015-0860	High		Off-by-one error in the extracthalf function in dpkg-deb/extract.c in the dpkg-deb component in Debian dpkg 1.16.x before 1.16.17 and 1.17.x before 1.17.26 allows remote attackers to execute arbitrary code via the archive magic version number in an old-style Debian binary package, which triggers a stack-based buffer overflow.	dpkg	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2208
6678	CVE-2015-0840	Medium		The dpkg-source command in Debian dpkg before 1.16.16 and 1.17.x before 1.17.25 allows remote attackers to bypass signature verification via a crafted Debian source control file (.dsc).	dpkg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-282
6679	CVE-2015-0797	Medium		GStreamer before 1.4.5, as used in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderbird before 31.7 on Linux, allows remote attackers to cause a denial of service (buffer over-read and application crash) or possibly execute arbitrary code via crafted H.264 video data in an m4v file.	gstreamer	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-366

	A	B	C	D	E	F	G	H	I	J	K	L	M
6680	CVE-2015-0794	High		modules.d/90crypt/module-setup.sh in the dracut package before 037-17.30.1 in openSUSE 13.2 allows local users to have unspecified impact via a symlink attack on /tmp/dracut_block_uuid.map.	dracut	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1916
6681	CVE-2015-0573	High	Critical	drivers/media/platform/msm/broadcast/tsc.c in the TSC driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (invalid pointer dereference) or possibly have unspecified other impact via a crafted application that makes a TSC_GET_CARD_STATUS ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1366
6682	CVE-2015-0568	High	High	Use-after-free vulnerability in the msm_set_crop function in drivers/media/video/msm/msm_camera.c in the MSM-Camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges or cause a denial of service (memory corruption) via an application that makes a crafted ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1434
6683	CVE-2015-0511	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : SP.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-329
6684	CVE-2015-0508	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB, a different vulnerability than CVE-2015-0506.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-325
6685	CVE-2015-0507	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-315
6686	CVE-2015-0506	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2015-0508.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-308
6687	CVE-2015-0505	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier, allows remote authenticated users to affect availability via vectors related to DDL.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-305
6688	CVE-2015-0503	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-311
6689	CVE-2015-0501	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Compiling.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-323
6690	CVE-2015-0500	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-333
6691	CVE-2015-0499	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.42 and earlier, and 5.6.23 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Federated.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-312
6692	CVE-2015-0498	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-319
6693	CVE-2015-0441	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Encryption.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-316
6694	CVE-2015-0439	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-341
6695	CVE-2015-0438	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-339
6696	CVE-2015-0433	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.41 and earlier, and 5.6.22 and earlier, allows remote authenticated users to affect availability via vectors related to InnoDB : DML.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-310
6697	CVE-2015-0432	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier allows remote authenticated users to affect availability via vectors related to Server : InnoDB : DDL : Foreign Key.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-144
6698	CVE-2015-0423	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-326
6699	CVE-2015-0411	High		Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier, and 5.6.21 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Server : Security : Encryption.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-113
6700	CVE-2015-0409	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.21 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-142
6701	CVE-2015-0405	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to XA.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-322
6702	CVE-2015-0391	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier, and 5.6.19 and earlier, allows remote authenticated users to affect availability via vectors related to DDL.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-116
6703	CVE-2015-0385	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.21 and earlier allows remote authenticated users to affect availability via unknown vectors related to Pluggable Auth.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-143
6704	CVE-2015-0382	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier and 5.6.21 and earlier allows remote attackers to affect availability via unknown vectors related to Server : Replication, a different vulnerability than CVE-2015-0381.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-145

	A	B	C	D	E	F	G	H	I	J	K	L	M
6705	CVE-2015-0381	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier and 5.6.21 and earlier allows remote attackers to affect availability via unknown vectors related to Server : Replication, a different vulnerability than CVE-2015-0382.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-132
6706	CVE-2015-0374	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier and 5.6.21 and earlier allows remote authenticated users to affect confidentiality via unknown vectors related to Server : Security : Privileges : Foreign Key.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-114
6707	CVE-2015-0361	High		Use-after-free vulnerability in Xen 4.2.x, 4.3.x, and 4.4.x allows remote domains to cause a denial of service (system crash) via a crafted hypercall during HVM guest teardown.CWE-416: Use After Free	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2289
6708	CVE-2015-0295	Medium		The BMP decoder in QtGui in QT before 5.5 does not properly calculate the masks used to extract the color components, which allows remote attackers to cause a denial of service (divide-by-zero and crash) via a crafted BMP file.	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-252
6709	CVE-2015-0293	Medium		The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-232
6710	CVE-2015-0292	High		Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-229
6711	CVE-2015-0291	Medium		The sigalgs implementation in t1_lib.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) by using an invalid signature_algorithms extension in the ClientHello message during a renegotiation.CWE-476: NULL Pointer Dereference	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-245
6712	CVE-2015-0290	Medium		The multi-block feature in the ssl3_write_bytes function in s3_pkt.c in OpenSSL 1.0.2 before 1.0.2a on 64-bit x86 platforms with AES NI support does not properly handle certain non-blocking I/O cases, which allows remote attackers to cause a denial of service (pointer corruption and application crash) via unspecified vectors.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-234
6713	CVE-2015-0289	Medium		The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.CWE-476: NULL Pointer Dereference	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-233
6714	CVE-2015-0288	Medium		The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.CWE-476: NULL Pointer Dereference	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-231
6715	CVE-2015-0287	Medium		The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-228
6716	CVE-2015-0286	Medium		The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-230
6717	CVE-2015-0285	Medium		The ssl3_client_hello function in s3_clnt.c in OpenSSL 1.0.2 before 1.0.2a does not ensure that the PRNG is seeded before proceeding with a handshake, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and then conducting a brute-force attack.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-244
6718	CVE-2015-0282	Medium		GnuTLS before 3.1.0 does not verify that the RSA PKCS #1 signature algorithm matches the signature algorithm in the certificate, which allows remote attackers to conduct downgrade attacks via unspecified vectors.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-240
6719	CVE-2015-0275	MEDIUM		A flaw was found in the way the Linux kernel's EXT4 filesystem handled page size > block size condition when fallocate zero range functionality is used	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-217
6720	CVE-2015-0274	High		The XFS implementation in the Linux kernel before 3.15 improperly uses an old size value during remote attribute replacement, which allows local users to cause a denial of service (transaction overrun and data corruption) or possibly gain privileges by leveraging XFS filesystem access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-249

	A	B	C	D	E	F	G	H	I	J	K	L	M
6721	CVE-2015-0273	High		Multiple use-after-free vulnerabilities in ext/date/php_date.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allow remote attackers to execute arbitrary code via crafted serialized input containing a (1) R or (2) r type specifier in (a) DateTimeZone data handled by the php_date_timezone_initialize_from_hash function or (b) DateTime data handled by the php_date_initialize_from_hash function.CWE-416: Use After Free	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-267
6722	CVE-2015-0271	Medium		The log-viewing function in the Red Hat redhat-access-plugin before 6.0.3 for OpenStack Dashboard (horizon) allows remote attackers to read arbitrary files via a crafted path.Per this link this vulnerability requires authentication.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2343
6723	CVE-2015-0268	Medium		The vgic_v2_to_sgi function in arch/arm/vgic-v2.c in Xen 4.5.x, when running on ARM hardware with general interrupt controller (GIC) version 2, allows local guest users to cause a denial of service (host crash) by writing an invalid value to the GICD.SGIR register.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2324
6724	CVE-2015-0267	Low		The Red Hat module-setup.sh script for kexec-tools, as distributed in the kexec-tools before 2.0.7-19 packages in Red Hat Enterprise Linux, allows local users to write to arbitrary files via a symlink attack on a temporary file.CWE-61: UNIX Symbolic Link (Symlink) Following	kexec-tools	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-397
6725	CVE-2015-0261	High		Integer signedness error in the mobility_opt_print function in the IPv6 mobility printer in tcpdump before 4.7.2 allows remote attackers to cause a denial of service (out-of-bounds read and crash) or possibly execute arbitrary code via a negative length value.	tcpdump	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-238
6726	CVE-2015-0255	Medium		X.Org Server (aka xserver and xorg-server) before 1.16.3 and 1.17.x before 1.17.1 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (crash) via a crafted string length value in a XkbSetGeometry request.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-169
6727	CVE-2015-0253	Medium		The read_request_line function in server/protocol.c in the Apache HTTP Server 2.4.12 does not initialize the protocol structure member, which allows remote attackers to cause a denial of service (NULL pointer dereference and process crash) by sending a request that lacks a method to an installation that enables the INCLUDES filter and has an ErrorDocument 400 directive specifying a local URI.CWE-476: NULL Pointer Dereference	apache	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-653
6728	CVE-2015-0252	Medium		internal/XMLReader.cpp in Apache Xerces-C before 3.1.2 allows remote attackers to cause a denial of service (segmentation fault and crash) via crafted XML data.	Xerces-c	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-490
6729	CVE-2015-0251	Medium		The mod_dav_svn server in Subversion 1.5.0 through 1.7.19 and 1.8.0 through 1.8.11 allows remote authenticated users to spoof the svn:author property via a crafted v1 HTTP protocol request sequences.	subversion	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-277
6730	CVE-2015-0248	Medium		The (1) mod_dav_svn and (2) svnserve servers in Subversion 1.6.0 through 1.7.19 and 1.8.0 through 1.8.11 allow remote attackers to cause a denial of service (assertion failure and abort) via crafted parameter combinations related to dynamically evaluated revision numbers.	subversion	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-281
6731	CVE-2015-0247	Medium		Heap-based buffer overflow in openfs.c in the libext2fs library in e2fsprogs before 1.42.12 allows local users to execute arbitrary code via crafted block group descriptor data in a filesystem image.	e2fsprogs	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-197
6732	CVE-2015-0245	Low		D-Bus 1.4.x through 1.6.x before 1.6.30, 1.8.x before 1.8.16, and 1.9.x before 1.9.10 does not validate the source of ActivationFailure signals, which allows local users to cause a denial of service (activation failure error returned) by leveraging a race condition involving sending an ActivationFailure signal before systemd responds.	d-bus	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-203
6733	CVE-2015-0244			If any error occurred while the server was in the middle of reading a protocol message from the client, it could lose synchronization and incorrectly try to interpret part of the message's data as a new protocol message. An attacker able to submit crafted binary data within a command parameter might succeed in injecting his own SQL commands this way. Statement timeout and query cancellation are the most likely sources of errors triggering this scenario. Particularly vulnerable are applications that use a timeout and also submit arbitrary user-crafted data as binary query parameters. Disabling statement timeout will reduce, but not eliminate, the risk of exploit.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-579
6734	CVE-2015-0243			Errors in memory size tracking within the pgcrypto module permitted stack buffer overruns and improper dependence on the contents of uninitialized memory. The buffer overrun cases can crash the server, and we have not ruled out the possibility of attacks that lead to privilege escalation.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-577
6735	CVE-2015-0242	Medium		PostgreSQL includes a replacement implementation of printf and related functions. This code will overrun a stack buffer when formatting a floating point number (conversion specifiers e, E, f, F, g or G) with requested precision greater than about 500. This will crash the server, and we have not ruled out the possibility of attacks that lead to privilege escalation. A database user can trigger such a buffer overrun through the to_char() SQL function. While that is the only affected core PostgreSQL functionality, extension modules that use printf-family functions may be at risk as well.	postgresql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-427

	A	B	C	D	E	F	G	H	I	J	K	L	M
6736	CVE-2015-0241			When to_char() processes a numeric formatting template calling for a large number of digits, PostgreSQL would read past the end of a buffer. When processing a crafted timestamp formatting template, PostgreSQL would write past the end of a buffer. Either case could crash the server. We have not ruled out the possibility of attacks that lead to privilege escalation, though they seem unlikely.	postgresql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-430
6737	CVE-2015-0240	High		The Netlogon server implementation in smbd in Samba 3.5.x and 3.6.x before 3.6.25, 4.0.x before 4.0.25, 4.1.x before 4.1.17, and 4.2.x before 4.2.0rc5 performs a free operation on an uninitialized stack pointer, which allows remote attackers to execute arbitrary code via crafted Netlogon packets that use the ServerPasswordSet RPC API, as demonstrated by packets reaching the _netr_ServerPasswordSet function in rpc_server/netlogon/srv_netlog_nt.c.	samba	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-174
6738	CVE-2015-0239	Medium		The em_sysenter function in arch/x86/kvm/emulate.c in the Linux kernel before 3.18.5, when the guest OS lacks SYSENTER MSR initialization, allows guest OS users to gain guest OS privileges or cause a denial of service (guest OS crash) by triggering use of a 16-bit code segment for emulation of a SYSENTER instruction.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-213
6739	CVE-2015-0236	LOW		libvirt before 1.2.12 allow remote authenticated users to obtain the VNC password by using the VIR_DOMAIN_XML_SECURE flag with a crafted (1) snapshot to the virDomainSnapshotGetXMLDesc interface or (2) image to the virDomainSaveImageGetXMLDesc interface.	libvirt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-123
6740	CVE-2015-0235	High		Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka GHOST.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2788
6741	CVE-2015-0232	Medium		The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.CWE-824: Access of Uninitialized Pointer	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-129
6742	CVE-2015-0231	High		Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate numerical keys within the serialized properties of an object. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8142.CWE-416: Use After Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-128
6743	CVE-2015-0228	Medium		The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.	Apache	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-222
6744	CVE-2015-0210	Medium	Medium	wpa_supplicant 2.0-16 does not properly check certificate subject name, which allows remote attackers to cause a man-in-the-middle attack.	wpa_supplicant	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5317
6745	CVE-2015-0209	Medium		Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.CWE-416: Use After Free	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-227
6746	CVE-2015-0208	Medium		The ASN.1 signature-verification implementation in the rsa_item_verify function in crypto/rsa/rsa_ameth.c in OpenSSL 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted RSA PSS parameters to an endpoint that uses the certificate-verification feature.CWE-476: NULL Pointer Dereference	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-237
6747	CVE-2015-0207	Medium		The dtls1_listen function in d1_lib.c in OpenSSL 1.0.2 before 1.0.2a does not properly isolate the state information of independent data streams, which allows remote attackers to cause a denial of service (application crash) via crafted DTLS traffic, as demonstrated by DTLS 1.0 traffic to a DTLS 1.2 server.CWE-476: NULL Pointer Dereference	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-257
6748	CVE-2015-0206	Medium		Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-95
6749	CVE-2015-0205	Medium		The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-85

	A	B	C	D	E	F	G	H	I	J	K	L	M
6750	CVE-2015-0204	Medium		The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-89
6751	CVE-2015-0203			The qpidd broker in Apache Qpid 0.30 and earlier allows remote authenticated users to cause a denial of service (daemon crash) via an AMQP message with (1) an invalid range in a sequence set, (2) content-bearing methods other than message-transfer, or (3) a session-gap control before a corresponding session-attach.	qpid	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3376
6752	CVE-2015-0202	High		The mod_dav_svn server in Subversion 1.8.0 through 1.8.11 allows remote attackers to cause a denial of service (memory consumption) via a large number of REPORT requests, which trigger the traversal of FSFS repository nodes.	subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-290
6753	CVE-2014-9984			nscd in the GNU C Library (aka glibc or libc6) before version 2.20 does not correctly compute the size of an internal buffer when processing netgroup requests, possibly leading to an nscd daemon crash or code execution as the user running nscd.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4430
6754	CVE-2014-9940	High	High	The regulator_ena_gpio_free function in drivers/regulator/core.c in the Linux kernel before 3.19 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4199
6755	CVE-2014-9939	High		ihex.c in GNU Binutils before 2.26 contains a stack buffer overflow when printing bad bytes in Intel Hex objects.	binutils	Unchanged	8.0.0.17	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3662
6756	CVE-2014-9938	Medium		contrib/completion/git-prompt.sh in Git before 1.9.3 does not sanitize branch names in the PS1 variable, allowing a malicious repository to cause code execution.	git	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3700
6757	CVE-2014-9922	High		The eCryptfs subsystem in the Linux kernel before 3.18 allows local users to gain privileges via a large filesystem stack that includes an overlayfs layer, related to fs/ecryptfs/main.c and fs/overlayfs/super.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-3919
6758	CVE-2014-9915	Medium		Off-by-one error in ImageMagick before 6.6.0-4 allows remote attackers to cause a denial of service (application crash) via a crafted 8BIM profile.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3661
6759	CVE-2014-9914	HIGH	High	Race condition in the ip4_datagram_release_cb function in net/ipv4/datagram.c in the Linux kernel before 3.15.2 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging incorrect expectations about locking during multithreaded access to internal data structures for IPv4 UDP sockets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3320
6760	CVE-2014-9913	Low	Medium	Buffer overflow in the list_files function in list.c in Info-Zip UnZip 6.0 allows remote attackers to cause a denial of service (crash) via vectors related to the compression method.	unzip	Unchanged	8.0.0.15	9.0.0.4	10.0.0.0	10.18.44.1	10.19.45.1	Not vulnerable	LIN9-3263
6761	CVE-2014-9912	High	Critical	The get_icu_disp_value_src_php function in ext/intl/locale/locale_methods.c in PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU uresbund.cpp component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a locale_get_display_name call with a long first argument.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2971
6762	CVE-2014-9907	Medium	Medium	coders/dds.c in ImageMagick allows remote attackers to cause a denial of service via a crafted DDS file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4137
6763	CVE-2014-9904	High		The snd_compress_check_input function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.17 does not properly check for an integer overflow, which allows local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call.CWE-190: Integer Overflow or Wraparound	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-941
6764	CVE-2014-9903	Low		The sched_read_attr function in kernel/sched/core.c in the Linux kernel 3.14-rc before 3.14-rc4 uses an incorrect size, which allows local users to obtain sensitive information from kernel stack memory via a crafted sched_getattr system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-918
6765	CVE-2014-9900	Medium		The ethtool_get_wol function in net/core/ethtool.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not initialize a certain data structure, which allows local users to obtain sensitive information via a crafted application, aka Android internal bug 28803952 and Qualcomm internal bug CR570754.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1418
6766	CVE-2014-9895	Medium		drivers/media/media-device.c in the Linux kernel before 3.11, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly initialize certain data structures, which allows local users to obtain sensitive information via a crafted application, aka Android internal bug 28750150 and Qualcomm internal bug CR570757, a different vulnerability than CVE-2014-1739.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1421
6767	CVE-2014-9892	Medium		The snd_compr_tstamp function in sound/core/compress_offload.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly initialize a timestamp data structure, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28770164 and Qualcomm internal bug CR568717.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1433

	A	B	C	D	E	F	G	H	I	J	K	L	M
6768	CVE-2014-9888	High		arch/arm/mm/dma-mapping.c in the Linux kernel before 3.13 on ARM platforms, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not prevent executable DMA mappings, which might allow local users to gain privileges via a crafted application, aka Android internal bug 28803642 and Qualcomm internal bug CR642735.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1394
6769	CVE-2014-9870	High		The Linux kernel before 3.11 on ARM platforms, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly consider user-space access to the TPIDRURW register, which allows local users to gain privileges via a crafted application, aka Android internal bug 28749743 and Qualcomm internal bug CR561044.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1403
6770	CVE-2014-9854	Medium		coders/tiff.c in ImageMagick allows remote attackers to cause a denial of service (application crash) via vectors related to the identification of image.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3720
6771	CVE-2014-9853	Medium		Memory leak in coders/rle.c in ImageMagick allows remote attackers to cause a denial of service (memory consumption) via a crafted rle file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3796
6772	CVE-2014-9852	High		distribute-cache.c in ImageMagick re-uses objects after they have been destroyed, which allows remote attackers to have unspecified impact via unspecified vectors.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3749
6773	CVE-2014-9851	Medium		ImageMagick 6.8.9.9 allows remote attackers to cause a denial of service (application crash).	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3807
6774	CVE-2014-9850	Medium		Logic error in ImageMagick 6.8.9.9 allows remote attackers to cause a denial of service (resource consumption).	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3668
6775	CVE-2014-9849	Medium		The png coder in ImageMagick allows remote attackers to cause a denial of service (crash).	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3797
6776	CVE-2014-9848	Medium		Memory leak in ImageMagick allows remote attackers to cause a denial of service (memory consumption).	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3764
6777	CVE-2014-9847	High		The jng decoder in ImageMagick 6.8.9.9 allows remote attackers to have an unspecified impact.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3773
6778	CVE-2014-9846	High		Buffer overflow in the ReadRLEImage function in coders/rle.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3676
6779	CVE-2014-9845	Medium		The ReadDIBImage function in coders/dib.c in ImageMagick allows remote attackers to cause a denial of service (crash) via a corrupted dib file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3775
6780	CVE-2014-9844	Medium		The ReadRLEImage function in coders/rle.c in ImageMagick 6.8.9.9 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3683
6781	CVE-2014-9843	High		The DecodePSDPixels function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact via unknown vectors.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3666
6782	CVE-2014-9842	Medium		Memory leak in the ReadPSDLayers function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3695
6783	CVE-2014-9841	High		The ReadPSDLayers function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact via unknown vectors, related to throwing of exceptions.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3719
6784	CVE-2014-9840	Medium		ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted palm file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3767
6785	CVE-2014-9839	Medium		magick/colormap-private.h in ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds access).	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3804
6786	CVE-2014-9838	Medium		magick/cache.c in ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service (crash).	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3689
6787	CVE-2014-9837	Medium	Medium	coders/pnm.c in ImageMagick 6.9.0-1 Beta and earlier allows remote attackers to cause a denial of service (crash) via a crafted png file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4121
6788	CVE-2014-9836	Medium		ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service via a crafted xpm file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3798
6789	CVE-2014-9835	Medium		Heap overflow in ImageMagick 6.8.9-9 via a crafted wpf file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3746
6790	CVE-2014-9834	Medium		Heap overflow in ImageMagick 6.8.9-9 via a crafted pict file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3744
6791	CVE-2014-9833	Medium		Heap overflow in ImageMagick 6.8.9-9 via a crafted psd file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3654
6792	CVE-2014-9832	Medium		Heap overflow in ImageMagick 6.8.9-9 via a crafted pcx file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3658
6793	CVE-2014-9831	Medium	High	coders/wpg.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted wpg file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5010
6794	CVE-2014-9830	Medium	High	coders/sun.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted sun file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5023
6795	CVE-2014-9829	Medium		coders/sun.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted sun file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3930
6796	CVE-2014-9828	Medium	High	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact via a crafted psd file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4960
6797	CVE-2014-9827	Medium	High	coders/xpm.c in ImageMagick allows remote attackers to have unspecified impact via a crafted xpm file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4936
6798	CVE-2014-9826	High		ImageMagick allows remote attackers to have unspecified impact via vectors related to error handling in sun files.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3948
6799	CVE-2014-9825	Medium		Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted psd file, a different vulnerability than CVE-2014-9824.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3884
6800	CVE-2014-9824	Medium		Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted psd file, a different vulnerability than CVE-2014-9825.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3905
6801	CVE-2014-9823	Medium		Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted palm file, a different vulnerability than CVE-2014-9819.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3962
6802	CVE-2014-9822	Medium		Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted quantum file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3885
6803	CVE-2014-9821	Medium		Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted xpm file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3898

	A	B	C	D	E	F	G	H	I	J	K	L	M
6804	CVE-2014-9820	Medium		Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted pnm file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3927
6805	CVE-2014-9819	Medium		Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted palm file, a different vulnerability than CVE-2014-9823.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3966
6806	CVE-2014-9818	Medium		ImageMagick allows remote attackers to cause a denial of service (out-of-bounds access) via a malformed sun file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3907
6807	CVE-2014-9817	Medium		Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted pdb file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3894
6808	CVE-2014-9816	Medium		ImageMagick allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted viff file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3901
6809	CVE-2014-9815	Medium		ImageMagick allows remote attackers to cause a denial of service (application crash) via a crafted wpg file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3920
6810	CVE-2014-9814	Medium		ImageMagick allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted wpg file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3882
6811	CVE-2014-9813	Medium		ImageMagick allows remote attackers to cause a denial of service (application crash) via a crafted viff file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3967
6812	CVE-2014-9812	Medium		ImageMagick allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted ps file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3877
6813	CVE-2014-9811	Medium		The xwd file handler in ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a malformed xwd file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3906
6814	CVE-2014-9810	Medium		The dpx file handler in ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a malformed dpx file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3943
6815	CVE-2014-9809	Medium		ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted xwd image.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3883
6816	CVE-2014-9808	Medium		ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted dpc image.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3940
6817	CVE-2014-9807	Medium		The pdb coder in ImageMagick allows remote attackers to cause a denial of service (double free) via unspecified vectors.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3915
6818	CVE-2014-9806	Medium		ImageMagick allows remote attackers to cause a denial of service (file descriptor consumption) via a crafted file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3923
6819	CVE-2014-9805	Medium		ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted pnm file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3916
6820	CVE-2014-9804	Medium		vision.c in ImageMagick allows remote attackers to cause a denial of service (infinite loop) via vectors related to too many object.CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3925
6821	CVE-2014-9803	High		arch/arm64/include/asm/pgtable.h in the Linux kernel before 3.15-rc5-next-20140519, as used in Android before 2016-07-05 on Nexus 5X and 6P devices, mishandles execute-only pages, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28557020.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1110
6822	CVE-2014-9771	MEDIUM		Integer overflow in imlib2 before 1.4.7 allows remote attackers to cause a denial of service (memory consumption or application crash) via a crafted image, which triggers an invalid read operation.	imlib2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-667
6823	CVE-2014-9770	LOW		tmpfiles.d/systemd.conf in systemd before 214 uses weak permissions for journal files under (1) /run/log/journal/%m and (2) /var/log/journal/%m, which allows local users to obtain sensitive information by reading these files.	systemd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-495
6824	CVE-2014-9769	High		pcre_jit_compile.c in PCRE 8.35 does not properly use table jumps to optimize nested alternatives, which allows remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via a crafted string, as demonstrated by packets encountered by Suricata during use of a regular expression in an Emerging Threats Open ruleset.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-440
6825	CVE-2014-9767	Medium		Directory traversal vulnerability in the ZipArchive::extractTo function in ext/zip/php_zip.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 and ext/zip/ext_zip.cpp in HHVM before 3.12.1 allows remote attackers to create arbitrary empty directories via a crafted ZIP archive.	php	Unchanged	8.0.0.6	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-760
6826	CVE-2014-9766	High		Integer overflow in the create_bits function in pixman-bits-image.c in Pixman before 0.32.6 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via large height and stride values.	pixman	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-475
6827	CVE-2014-9765	Medium		Buffer overflow in the main_get_appheader function in xdelta3-main.h in xdelta3 before 3.0.9 allows remote attackers to execute arbitrary code via a crafted input file.	xdelta3	Unchanged	8.0.0.6	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-484
6828	CVE-2014-9764	MEDIUM		imlib2 before 1.4.7 allows remote attackers to cause a denial of service (segmentation fault) via a crafted GIF file.	imlib2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-557
6829	CVE-2014-9763	MEDIUM		imlib2 before 1.4.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted PNM file.	imlib2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-620
6830	CVE-2014-9762	MEDIUM		imlib2 before 1.4.7 allows remote attackers to cause a denial of service (segmentation fault) via a GIF image without a colormap.	imlib2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-578
6831	CVE-2014-9761	HIGH		A stack overflow (unbounded alloca) can cause applications which process long strings with the nan function to crash or, potentially, execute arbitrary code.	glibc	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-235
6832	CVE-2014-9756	Medium		The psf_fwrite function in file_io.c in libsndfile allows attackers to cause a denial of service (divide-by-zero error and application crash) via unspecified vectors related to the headindex variable.	libsndfile	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1897

	A	B	C	D	E	F	G	H	I	J	K	L	M
6833	CVE-2014-9751	Medium		The read_network_packet function in ntp_io.c in ntpd in NTP 4.x before 4.2.8p1 on Linux and OS X does not properly determine whether a source IP address is an IPv6 loopback address, which makes it easier for remote attackers to spoof restricted packets, and read or write to the runtime state, by leveraging the ability to reach the ntpd machine's network interface with a packet from the ::1 address.	ntp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN8-1085
6834	CVE-2014-9750	Medium		ntp_crypto.c in ntpd in NTP 4.x before 4.2.8p1, when Autokey Authentication is enabled, allows remote attackers to obtain sensitive information from process memory or cause a denial of service (daemon crash) via a packet containing an extension field with an invalid value for the length of its value field.	ntp	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN8-1091
6835	CVE-2014-9749	Medium		Squid 3.4.4 through 3.4.11 and 3.5.0.1 through 3.5.1, when Digest authentication is used, allow remote authenticated users to retain access by leveraging a stale nonce, aka Nonce replay vulnerability.	squid	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-1582
6836	CVE-2014-9747	Medium		The t42_parse_encoding function in type42/t42parse.c in FreeType before 2.5.4 does not properly update the current position for immediates-only mode, which allows remote attackers to cause a denial of service (infinite loop) via a Type42 font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-822
6837	CVE-2014-9746	High		The (1) t1_parse_font_matrix function in type1/t1load.c, (2) cid_parse_font_matrix function in cid/cidload.c, (3) t42_parse_font_matrix function in type42/t42parse.c, and (4) ps_parser_load_field function in psaux/psobjs.c in FreeType before 2.5.4 do not check return values, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-826
6838	CVE-2014-9745	Medium		The parse_encoding function in type1/t1load.c in FreeType before 2.5.3 allows remote attackers to cause a denial of service (infinite loop) via a broken number-with-base in a Postscript stream, as demonstrated by 8#garbage.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-973
6839	CVE-2014-9744	High		Memory leak in PolarSSL before 1.3.9 allows remote attackers to cause a denial of service (memory consumption) via a large number of ClientHello messages. NOTE: this identifier was SPLIT from CVE-2014-8628 per ADT3 due to different affected versions.	polarssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-772
6840	CVE-2014-9731	Low		The UDF filesystem implementation in the Linux kernel before 3.18.2 does not ensure that space is available for storing a symlink target's name along with a trailing \0 character, which allows local users to obtain sensitive information via a crafted filesystem image, related to fs/udf/symlink.c and fs/udf/unicode.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-205
6841	CVE-2014-9730	Medium		The udf_pc_to_char function in fs/udf/symlink.c in the Linux kernel before 3.18.2 relies on component lengths that are unused, which allows local users to cause a denial of service (system crash) via a crafted UDF filesystem image.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-201
6842	CVE-2014-9729	Medium		The udf_read_inode function in fs/udf/inode.c in the Linux kernel before 3.18.2 does not ensure a certain data-structure size consistency, which allows local users to cause a denial of service (system crash) via a crafted UDF filesystem image.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-203
6843	CVE-2014-9728	Medium		The UDF filesystem implementation in the Linux kernel before 3.18.2 does not validate certain lengths, which allows local users to cause a denial of service (buffer over-read and system crash) via a crafted filesystem image, related to fs/udf/inode.c and fs/udf/symlink.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-211
6844	CVE-2014-9718	Medium		The (1) BMDMA and (2) AHCI HBA interfaces in the IDE functionality in QEMU 1.0 through 2.1.3 have multiple interpretations of a function's return value, which allows guest OS users to cause a host OS denial of service (memory consumption or infinite loop, and system crash) via a PRDT with zero complete sectors, related to the bmdma_prepare_buf and ahci_dma_prepare_buf functions.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-320
6845	CVE-2014-9717	Low		fs/namespace.c in the Linux kernel before 4.0.2 processes MNT_DETACH umount2 system calls without verifying that the MNT_LOCKED flag is unset, which allows local users to bypass intended access restrictions and navigate to filesystem locations beneath a mount by calling umount2 within a user namespace.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-652
6846	CVE-2014-9715	Medium		include/net/netfilter/ nf_conntrack_extend.h in the netfilter subsystem in the Linux kernel before 3.14.5 uses an insufficiently large data type for certain extension data, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via outbound network traffic that triggers extension loading, as demonstrated by configuring a PPTP tunnel in a NAT environment.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-387
6847	CVE-2014-9713	Medium		The default slapd configuration in the Debian openldap package 2.4.23-3 through 2.4.39-1.1 allows remote authenticated users to modify the user's permissions and other user attributes via unspecified vectors.	openldap	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-272
6848	CVE-2014-9710	Medium		The Btrfs implementation in the Linux kernel before 3.19 does not ensure that the visible xattr state is consistent with a requested replacement, which allows local users to bypass intended ACL settings and gain privileges via standard filesystem operations (1) during an xattr-replacement time window, related to a race condition, or (2) after an xattr-replacement attempt that fails because the data does not fit.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-396

	A	B	C	D	E	F	G	H	I	J	K	L	M
6849	CVE-2014-9709	Medium		The GetCode_ function in gd_gif_in.c in GD 2.1.1 and earlier, as used in PHP before 5.5.21 and 5.6.x before 5.6.5, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted GIF image that is improperly handled by the gdImageCreateFromGif function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-283
6850	CVE-2014-9705	High		Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-276
6851	CVE-2014-9684	Medium		OpenStack Image Registry and Delivery Service (Glance) 2014.2 through 2014.2.2 does not properly remove images, which allows remote authenticated users to cause a denial of service (disk consumption) by creating a large number of images using the task v2 API and then deleting them before the uploads finish, a different vulnerability than CVE-2015-1881.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2323
6852	CVE-2014-9683	Low		Off-by-one error in the ecryptfs_decode_from_filename function in fs/ecryptfs/crypto.c in the eCryptfs subsystem in the Linux kernel before 3.18.2 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted filename.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-214
6853	CVE-2014-9680			sudo before 1.8.12 does not ensure that the TZ environment variable is associated with a zoneinfo file, which allows local users to open arbitrary files for read access (but not view file contents) by running a program within an sudo session, as demonstrated by interfering with terminal output, discarding kernel-log messages, or repositioning tape drives.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4082
6854	CVE-2014-9679	Medium		Integer underflow in the cupsRasterReadPixels function in filter/raster.c in CUPS before 2.0.2 allows remote attackers to have unspecified impact via a malformed compressed raster file, which triggers a buffer overflow.	cups	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-186
6855	CVE-2014-9676	Medium		The seg_write_packet function in libavformat/segment.c in ffmpeg 2.1.4 and earlier does not free the correct memory location, which allows remote attackers to cause a denial of service (invalid memory handler) and possibly execute arbitrary code via a crafted video that triggers a use after free.CWE-416: Use After Free	gst-ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-216
6856	CVE-2014-9675	Medium		bdf/bdflib.c in FreeType before 2.5.4 identifies property names by only verifying that an initial substring is present, which allows remote attackers to discover heap pointer values and bypass the ASLR protection mechanism via a crafted BDF font.	freetype	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-172
6857	CVE-2014-9674	High		The Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.5.4 proceeds with adding to length values without validating the original values, which allows remote attackers to cause a denial of service (integer overflow and heap-based buffer overflow) or possibly have unspecified other impact via a crafted Mac font.CWE-190: Integer Overflow or Wraparound	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-196
6858	CVE-2014-9673	High		Integer signedness error in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.5.4 allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted Mac font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-188
6859	CVE-2014-9672	Medium		Array index error in the parse_fond function in base/ftmac.c in FreeType before 2.5.4 allows remote attackers to cause a denial of service (out-of-bounds read) or obtain sensitive information from process memory via a crafted FOND resource in a Mac font file.	freetype	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-184
6860	CVE-2014-9671	Medium		Off-by-one error in the pcf_get_properties function in pcf/pcfread.c in FreeType before 2.5.4 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted PCF file with a 0xffffffff size value that is improperly incremented.CWE-476: NULL Pointer Dereference	freetype	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-194
6861	CVE-2014-9670	Medium		Multiple integer signedness errors in the pcf_get_encodings function in pcf/pcfread.c in FreeType before 2.5.4 allow remote attackers to cause a denial of service (integer overflow, NULL pointer dereference, and application crash) via a crafted PCF file that specifies negative values for the first column and first row.	freetype	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-168
6862	CVE-2014-9669	High		Multiple integer overflows in sfnt/ttcmap.c in FreeType before 2.5.4 allow remote attackers to cause a denial of service (out-of-bounds read or memory corruption) or possibly have unspecified other impact via a crafted cmap SFNT table.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-166
6863	CVE-2014-9668	High		The woff_open_font function in sfnt/sfobjs.c in FreeType before 2.5.4 proceeds with offset+length calculations without restricting length values, which allows remote attackers to cause a denial of service (integer overflow and heap-based buffer overflow) or possibly have unspecified other impact via a crafted Web Open Font Format (WOFF) file.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-198
6864	CVE-2014-9667	High		sfnt/ttload.c in FreeType before 2.5.4 proceeds with offset+length calculations without restricting the values, which allows remote attackers to cause a denial of service (integer overflow and out-of-bounds read) or possibly have unspecified other impact via a crafted SFNT table.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-182

	A	B	C	D	E	F	G	H	I	J	K	L	M
6865	CVE-2014-9666	High		The tt_sbit_decoder_init function in sfnt/ttsbit.c in FreeType before 2.5.4 proceeds with a count-to-size association without restricting the count value, which allows remote attackers to cause a denial of service (integer overflow and out-of-bounds read) or possibly have unspecified other impact via a crafted embedded bitmap.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-190
6866	CVE-2014-9665	High		The Load_SBit_Png function in sfnt/pngshim.c in FreeType before 2.5.4 does not restrict the rows and pitch values of PNG data, which allows remote attackers to cause a denial of service (integer overflow and heap-based buffer overflow) or possibly have unspecified other impact by embedding a PNG file in a .ttf font file.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-177
6867	CVE-2014-9664	High		FreeType before 2.5.4 does not check for the end of the data during certain parsing actions, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted Type42 font, related to type42/t42parse.c and type1/t1load.c.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-191
6868	CVE-2014-9663	High		The tt_cmap4_validate function in sfnt/ttcmap.c in FreeType before 2.5.4 validates a certain length field before that field's value is completely calculated, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted cmap SFNT table.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-179
6869	CVE-2014-9662	High		cff/cf2ft.c in FreeType before 2.5.4 does not validate the return values of point-allocation functions, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted OTF font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-180
6870	CVE-2014-9661	High		type42/t42parse.c in FreeType before 2.5.4 does not consider that scanning can be incomplete without triggering an error, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted Type42 font.CWE-416: Use After Free	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-200
6871	CVE-2014-9660	High		The _bdf_parse_glyphs function in bdf/bdflib.c in FreeType before 2.5.4 does not properly handle a missing ENDCHAR record, which allows remote attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via a crafted BDF font.CWE-476: NULL Pointer Dereference	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-165
6872	CVE-2014-9659	High		cff/cf2intrp.c in the CFF CharString interpreter in FreeType before 2.5.4 proceeds with additional hints after the hint mask has been computed, which allows remote attackers to execute arbitrary code or cause a denial of service (stack-based buffer overflow) via a crafted OpenType font. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-2240.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-199
6873	CVE-2014-9658	High		The tt_face_load_kern function in sfnt/ttkern.c in FreeType before 2.5.4 enforces an incorrect minimum table length, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted TrueType font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-185
6874	CVE-2014-9657	High		The tt_face_load_hdmx function in truetype/ttpload.c in FreeType before 2.5.4 does not establish a minimum record size, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted TrueType font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-170
6875	CVE-2014-9656	High		The tt_sbit_decoder_load_image function in sfnt/ttsbit.c in FreeType before 2.5.4 does not properly check for an integer overflow, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted OpenType font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-195
6876	CVE-2014-9655	MEDIUM		libtiff: use of uninitialized memory in putcontig8bitYCbCr21tile and NeXTDecode	tiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-276
6877	CVE-2014-9654			The Regular Expressions package in International Components for Unicode (ICU) for C/C++ before 2014-12-03, as used in Google Chrome before 40.0.2214.91, calculates certain values without ensuring that they can be represented in a 24-bit field, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted string, a related issue to CVE-2014-7923.	icu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4113
6878	CVE-2014-9653	High		readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-274
6879	CVE-2014-9652	Medium		The mconvert function in softmagic.c in file before 5.21, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not properly handle a certain string-length field during a copy of a truncated version of a Pascal string, which might allow remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via a crafted file.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-266
6880	CVE-2014-9645			The add_probe function in modutils/modprobe.c in BusyBox before 1.23.0 allows local users to bypass intended restrictions on loading kernel modules via a / (slash) character in a module name, as demonstrated by an ifconfig /usbserial up command or a mount -t /snd_pcm none / command.	busybox	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3548

	A	B	C	D	E	F	G	H	I	J	K	L	M
6881	CVE-2014-9644	Low		The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bind system call for an AF_ALG socket with a parenthesized module template expression in the salg_name field, as demonstrated by the vfat(aes) expression, a different vulnerability than CVE-2013-7421.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-217
6882	CVE-2014-9637			GNU patch 2.7.2 and earlier allows remote attackers to cause a denial of service (memory consumption and segmentation fault) via a crafted diff file.	patch	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5155
6883	CVE-2014-9636	Medium		unzip 6.0 allows remote attackers to cause a denial of service (out-of-bounds read or write and crash) via an extra field with an uncompressed size smaller than the compressed field size in a zip archive that advertises STORED method compression.	unzip	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-164
6884	CVE-2014-9621	Medium		The ELF parser in file 5.16 through 5.21 allows remote attackers to cause a denial of service via a long string.	file	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-135
6885	CVE-2014-9620	Medium		The ELF parser in file 5.08 through 5.21 allows remote attackers to cause a denial of service via a large number of notes.	file	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-115
6886	CVE-2014-9604	High		libavcodec/utvideodec.c in FFmpeg before 2.5.2 does not check for a zero value of a slice height, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Ut Video data, related to the (1) restore_median and (2) restore_median_il functions.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-110
6887	CVE-2014-9603	High		The vmd_decode function in libavcodec/vmdvideo.c in FFmpeg before 2.5.2 does not validate the relationship between a certain length value and the frame width, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Sierra VMD video data.	gst-ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-120
6888	CVE-2014-9602	High		libavcodec/xface.h in FFmpeg before 2.5.2 establishes certain digits and words array dimensions that do not satisfy a required mathematical relationship, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted X-Face image data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-117
6889	CVE-2014-9585	Low		The vdso_addr function in arch/x86/vdso/vma.c in the Linux kernel through 3.18.2 does not properly choose memory locations for the vDSO area, which makes it easier for local users to bypass the ASLR protection mechanism by guessing a location at the end of a PMD.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-93
6890	CVE-2014-9584	Low		The parse_rock_ridge_inode_internal function in fs/isofs/rock.c in the Linux kernel before 3.18.2 does not validate a length value in the Extensions Reference (ER) System Use Field, which allows local users to obtain sensitive information from kernel memory via a crafted iso9660 image.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-88
6891	CVE-2014-9529	High		Race condition in the key_gc_unused_keys function in security/keys/gc.c in the Linux kernel through 3.18.2 allows local users to cause a denial of service (memory corruption or panic) or possibly have unspecified other impact via keyctl commands that trigger access to a key structure member during garbage collection of a key.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-98
6892	CVE-2014-9512	Medium		rsync 3.1.1 allows remote attackers to write to arbitrary files via a symlink attack on a file in the synchronization path.	rsync	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-205
6893	CVE-2014-9497	Medium	High	Buffer overflow in mpg123 before 1.18.0.	mpg123	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5217
6894	CVE-2014-9496	High		The sd2_parse_rsrc_fork function in sd2.c in libsndfile allows attackers to have unspecified impact via vectors related to a (1) map offset or (2) rsrc marker, which triggers an out-of-bounds read.	libsndfile	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-138
6895	CVE-2014-9495	High		Heap-based buffer overflow in the png_combine_row function in libpng before 1.5.21 and 1.6.x before 1.6.16 might allow context-dependent attackers to execute arbitrary code via a very wide interlaced PNG image.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-97
6896	CVE-2014-9488	HIGH		The is_utf8_well_formed function in GNU less before 475 allows remote attackers to have unspecified impact via malformed UTF-8 characters, which triggers an out-of-bounds read.	less	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-284
6897	CVE-2014-9483	Medium	High	Emacs 24.4 allows remote attackers to bypass security restrictions.	emacs	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5389
6898	CVE-2014-9474			Buffer overflow in the mpfr_strtofr function in GNU MPFR before 3.1.2-p11 allows context-dependent attackers to have unspecified impact via vectors related to incorrect documentation for mpn_set_str.	mpfr	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5597
6899	CVE-2014-9471	High		The parse_datetime function in GNU coreutils allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted date string, as demonstrated by the --date=TZ=123345 @1 string to the touch or date command.	coreutils	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-134
6900	CVE-2014-9462	High		The _validaterepo function in sshpeer in Mercurial before 3.2.4 allows remote attackers to execute arbitrary commands via a crafted repository name in a clone command.	mercurial	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-294
6901	CVE-2014-9447	Medium		Directory traversal vulnerability in the read_long_names function in libelf/elf_begin.c in elfutils 0.152 and 0.161 allows remote attackers to write to arbitrary files to the root directory via a / (slash) in a crafted archive, as demonstrated using the ar program.	elfutils	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-83
6902	CVE-2014-9428	High		The batadv_frag_merge_packets function in net/batman-adv/fragmentation.c in the B.A.T.M.A.N. implementation in the Linux kernel through 3.18.1 uses an incorrect length field during a calculation of an amount of memory, which allows remote attackers to cause a denial of service (mesh-node system crash) via fragmented packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-84

	A	B	C	D	E	F	G	H	I	J	K	L	M
6903	CVE-2014-9427	High		sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.	php	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-86
6904	CVE-2014-9426	High		** DISPUTED ** The apprentice_load function in libmagic/apprentice.c in the Fileinfo component in PHP through 5.6.4 attempts to perform a free operation on a stack-based character array, which allows remote attackers to cause a denial of service (memory corruption or application crash) or possibly have unspecified other impact via unknown vectors. NOTE: this is disputed by the vendor because the standard erealloc behavior makes the free operation unreachable.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-87
6905	CVE-2014-9425	High		Double free vulnerability in the zend_ts_hash_graceful_destroy function in zend_ts_hash.c in the Zend Engine in PHP through 5.5.20 and 5.6.x through 5.6.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.CWE-415: Double Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-94
6906	CVE-2014-9423	Medium		The svcauth_gss_accept_sec_context function in lib/rpc/svc_auth_gss.c in MIT Kerberos 5 (aka krb5) 1.11.x through 1.11.5, 1.12.x through 1.12.2, and 1.13.x before 1.13.1 transmits uninitialized interposer data to clients, which allows remote attackers to obtain sensitive information from process heap memory by sniffing the network for data in a handle field.	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-204
6907	CVE-2014-9422	Medium		The check_rpcsec_auth function in kadmin/server/kadm_rpc_svc.c in kadmind in MIT Kerberos 5 (aka krb5) through 1.11.5, 1.12.x through 1.12.2, and 1.13.x before 1.13.1 allows remote authenticated users to bypass a kadmin/* authorization check and obtain administrative access by leveraging access to a two-component principal with an initial kadmind substring, as demonstrated by a ka/x principal.	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-175
6908	CVE-2014-9421	High		The auth_gssapi_unwrap_data function in lib/rpc/auth_gssapi_misc.c in MIT Kerberos 5 (aka krb5) through 1.11.5, 1.12.x through 1.12.2, and 1.13.x before 1.13.1 does not properly handle partial XDR deserialization, which allows remote authenticated users to cause a denial of service (use-after-free and double free, and daemon crash) or possibly execute arbitrary code via malformed XDR data, as demonstrated by data sent to kadmind.CWE-416: Use After Free	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-173
6909	CVE-2014-9420	Medium		The rock_continue function in fs/isofs/rock.c in the Linux kernel through 3.18.1 does not restrict the number of Rock Ridge continuation entries, which allows local users to cause a denial of service (infinite loop, and system crash or hang) via a crafted iso9660 image.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2566
6910	CVE-2014-9419	Low		The __switch_to function in arch/x86/kernel/process_64.c in the Linux kernel through 3.18.1 does not ensure that Thread Local Storage (TLS) descriptors are loaded before proceeding with other steps, which makes it easier for local users to bypass the ASLR protection mechanism via a crafted application that reads a TLS base address.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2567
6911	CVE-2014-9410	High		The vfe31_proc_general function in drivers/media/video/msm/vfe/msm_vfe31.c in the MSM-VFE31 driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not validate a certain id value, which allows attackers to gain privileges or cause a denial of service (memory corruption) via an application that makes a crafted ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1399
6912	CVE-2014-9403	Medium		The CWebAdminMod::ChanPage function in modules/webadmin.cpp in ZNC before 1.4 allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) by adding a channel with the same name as an existing channel but without the leading # character, related to a use-after-delete error.CWE-476: NULL Pointer Dereference	znc	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2571
6913	CVE-2014-9402	High		The nss_dns implementation of getnetbyname in GNU C Library (aka glibc) before 2.21, when the DNS backend in the Name Service Switch configuration is enabled, allows remote attackers to cause a denial of service (infinite loop) by sending a positive answer while a network name is being process.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-178
6914	CVE-2014-9365	Medium		The HTTP clients in the (1) httplib, (2) urllib, (3) urllib2, and (4) xmlrpclib libraries in CPython (aka Python) 2.x before 2.7.9 and 3.x before 3.4.3, when accessing an HTTPS URL, do not (a) check the certificate against a trust store or verify that the server hostname matches a domain name in the subject's (b) Common Name or (c) subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.CWE-295: Improper Certificate Validation	python	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2444

	A	B	C	D	E	F	G	H	I	J	K	L	M
6915	CVE-2014-9330	Medium		Integer overflow in tif_packbits.c in bmp2tif in libtiff 4.0.3 allows remote attackers to cause a denial of service (crash) via crafted BMP image, related to dimensions, which triggers an out-of-bounds read.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-125
6916	CVE-2014-9322	High		arch/x86/kernel/entry_64.S in the Linux kernel before 3.17.5 does not properly handle faults associated with the Stack Segment (SS) segment register, which allows local users to gain privileges by triggering an IRET instruction that leads to access to a GS Base address from the wrong space.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2573
6917	CVE-2014-9319	Medium		The ff_hevc_decode_nal_sps function in libavcodec/hevc_ps.c in FFMpeg before 2.1.6, 2.2.x through 2.3.x, and 2.4.x before 2.4.4 allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted .bit file.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2441
6918	CVE-2014-9318	High		The raw_decode function in libavcodec/rawdec.c in FFMpeg before 2.1.6, 2.2.x through 2.3.x, and 2.4.x before 2.4.4 allows remote attackers to cause a denial of service (out-of-bounds heap access) and possibly have other unspecified impact via a crafted .cine file that triggers the avpicture_get_size function to return a negative frame size.	gst-ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2433
6919	CVE-2014-9317	High		The decode_ihdr_chunk function in libavcodec/pngdec.c in FFMpeg before 2.1.6, 2.2.x through 2.3.x, and 2.4.x before 2.4.4 allows remote attackers to cause a denial of service (out-of-bounds heap access) and possibly have other unspecified impact via an IDAT before an IHDR in a PNG file.	gst-ffmpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2419
6920	CVE-2014-9316	High		The mjpeg_decode_app function in libavcodec/mjpegdec.c in FFMpeg before 2.1.6, 2.2.x through 2.3.x, and 2.4.x before 2.4.4 allows remote attackers to cause a denial of service (out-of-bounds heap access) and possibly have other unspecified impact via vectors related to LJIF tags in an MJPEG file.	gst-ffmpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2415
6921	CVE-2014-9298			Sec issue 2672 of NTP: On some OSes ::1 can be spoofed, bypassing source IP ACLs.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-264
6922	CVE-2014-9297			Sec bug 2671 of NTP: vallen in extension fields are not validated.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-263
6923	CVE-2014-9296	Medium		The receive function in ntp_proto.c in ntpd in NTP before 4.2.8 continues to execute after detecting a certain authentication error, which might allow remote attackers to trigger an unintended association change via crafted packets.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2502
6924	CVE-2014-9295	High		Multiple stack-based buffer overflows in ntpd in NTP before 4.2.8 allow remote attackers to execute arbitrary code via a crafted packet, related to (1) the crypto_recv function when the Autokey Authentication feature is used, (2) the ctl_putdata function, and (3) the configure function.	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2501
6925	CVE-2014-9294	High		util/ntp-keygen.c in ntp-keygen in NTP before 4.2.7p230 uses a weak RNG seed, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2500
6926	CVE-2014-9293	High		The config_auth function in ntpd in NTP before 4.2.7p11, when an auth key is not configured, improperly generates a key, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.CWE-332: Insufficient Entropy in PRNG	ntp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2498
6927	CVE-2014-9278	Medium		The OpenSSH server, as used in Fedora and Red Hat Enterprise Linux 7 and when running in a Kerberos environment, allows remote authenticated users to log in as another user when they are listed in the .k5users file of that user, which might bypass intended authentication requirements that would force a local login.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2432
6928	CVE-2014-9221	Medium		strongSwan 4.5.x through 5.2.x before 5.2.1 allows remote attackers to cause a denial of service (invalid pointer dereference) via a crafted IKEv2 Key Exchange (KE) message with Diffie-Hellman (DH) group 1025.	strongswan	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-96
6929	CVE-2014-9219	Medium		Cross-site scripting (XSS) vulnerability in the redirection feature in url.php in phpMyAdmin 4.2.x before 4.2.13.1 allows remote attackers to inject arbitrary web script or HTML via the url parameter.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2443
6930	CVE-2014-9218	Medium		libraries/common.inc.php in phpMyAdmin 4.0.x before 4.0.10.7, 4.1.x before 4.1.14.8, and 4.2.x before 4.2.13.1 allows remote attackers to cause a denial of service (resource consumption) via a long password.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2414
6931	CVE-2014-9140	Medium		Buffer overflow in the ppp_hdlc function in print-ppp.c in tcpdump 4.6.2 and earlier allows remote attackers to cause a denial of service (crash) cia a crafted PPP packet.	tcpdump	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2409
6932	CVE-2014-9130	Medium		scanner.c in LibYAML 0.1.5 and 0.1.6, as used in the YAML-LibYAML (aka YAML-XS) module for Perl, allows context-dependent attackers to cause a denial of service (assertion failure and crash) via vectors involving line-wrapping.	libyaml	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2410
6933	CVE-2014-9114			Sebastian Krahmer reported a command injection flaw in blkid. This could possibly result in command execution with root privileges (for example, when running blkid on a malicious USB drive)	util-linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-358
6934	CVE-2014-9112	Medium		Heap-based buffer overflow in the process_copy_in function in GNU Cpio 2.11 allows remote attackers to cause a denial of service via a large block value in a cpio archive.	cpio	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2411
6935	CVE-2014-9092			libjpeg-turbo before 1.3.1 allows remote attackers to cause a denial of service (crash) via a crafted JPEG file, related to the Exif marker.	libjpeg-turbo	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5590

	A	B	C	D	E	F	G	H	I	J	K	L	M
6936	CVE-2014-9090	MEDIUM		The do_double_fault function in arch/x86/kernel/traps.c in the Linux kernel through 3.17.4 does not properly handle faults associated with the Stack Segment (SS) segment register, which allows local users to cause a denial of service (panic) via a modify_ldt system call, as demonstrated by sigreturn_32 in the linux-clock-tests test suite.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2111
6937	CVE-2014-9066	Medium		Xen 4.4.x and earlier, when using a large number of VCPUs, does not properly handle read and write locks, which allows local x86 guest users to cause a denial of service (write denial or NMI watchdog timeout and host crash) via a large number of read request, a different vulnerability than CVE-2014-9065.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2259
6938	CVE-2014-9065	Medium		common/spinlock.c in Xen 4.4.x and earlier does not properly handle read and write locks, which allows local x86 guest users to cause a denial of service (write denial or NMI watchdog timeout and host crash) via a large number of read requests, a different vulnerability to CVE-2014-9066.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2262
6939	CVE-2014-9030	High		The do_mmu_update function in arch/x86/mm.c in Xen 3.2.x through 4.4.x does not properly manage page references, which allows remote domains to cause a denial of service by leveraging control over an HVM guest and a crafted MMU_MACHPHYS_UPDATE.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2224
6940	CVE-2014-9029	High		Multiple off-by-one errors in the (1) jpc_dec_cp_setfromcox and (2) jpc_dec_cp_setfromrgn functions in jpc/jpc_dec.c in JasPer 1.900.1 and earlier allow remote attackers to execute arbitrary code via a crafted jp2 file, which triggers a heap-based buffer overflow.	WRLinux doesn't ship jasper.	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-452
6941	CVE-2014-8989	MEDIUM		The Linux kernel through 3.17.4 does not properly restrict dropping of supplemental group memberships in certain namespace scenarios, which allows local users to bypass intended file permissions by leveraging a POSIX ACL containing an entry for the group category that is more restrictive than the entry for the other category, aka a negative groups issue, related to kernel/groups.c, kernel/uid16.c, and kernel/user_namespace.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2113
6942	CVE-2014-8961	MEDIUM		Directory traversal vulnerability in libraries/error_report.lib.php in the error-reporting feature in phpMyAdmin 4.1.x before 4.1.14.7 and 4.2.x before 4.2.12 allows remote authenticated users to obtain potentially sensitive information about a file's line count via a crafted parameter.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2166
6943	CVE-2014-8960	LOW		Cross-site scripting (XSS) vulnerability in libraries/error_report.lib.php in the error-reporting feature in phpMyAdmin 4.1.x before 4.1.14.7 and 4.2.x before 4.2.12 allows remote authenticated users to inject arbitrary web script or HTML via a crafted filename.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2128
6944	CVE-2014-8959	MEDIUM		Directory traversal vulnerability in libraries/gis/GIS_Factory.class.php in the GIS editor in phpMyAdmin 4.0.x before 4.0.10.6, 4.1.x before 4.1.14.7, and 4.2.x before 4.2.12 allows remote authenticated users to include and execute arbitrary local files via a crafted geometry-type parameter.	phpMyAdmin	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2155
6945	CVE-2014-8958	MEDIUM		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.6, 4.1.x before 4.1.14.7, and 4.2.x before 4.2.12 allow remote authenticated users to inject arbitrary web script or HTML via a crafted (1) database, (2) table, or (3) column name that is improperly handled during rendering of the table browse page; a crafted ENUM value that is improperly handled during rendering of the (4) table print view or (5) zoom search page; or (6) a crafted pma_fontsize cookie that is improperly handled during rendering of the home page.	phpMyAdmin	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2127
6946	CVE-2014-8884	MEDIUM		Stack-based buffer overflow in the ttusbdecfe_dvbs_diseqc_send_master_cmd function in drivers/media/usb/ttusb-dec/ttusbdecfe.c in the Linux kernel before 3.17.4 allows local users to cause a denial of service (system crash) or possibly gain privileges via a large message length in an ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2143
6947	CVE-2014-8867	Medium		The acceleration support for the REP MOVS instruction in Xen 4.4.x, 3.2.x, and earlier lacks properly bounds checking for memory mapped I/O (MMIO) emulated in the hypervisor, which allows local HVM guests to cause a denial of service (host crash) via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2260
6948	CVE-2014-8866	Medium		The compatibility mode hypercall argument translation in Xen 3.3.x through 4.4.x, when running on a 64-bit hypervisor, allows local 32-bit HVM guests to cause a denial of service (host crash) via vectors involving altering the high halves of registers while in 64-bit mode.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2265
6949	CVE-2014-8769	Medium		tcpdump 3.8 through 4.6.2 might allow remote attackers to obtain sensitive information from memory or cause a denial of service (packet loss or segmentation fault) via a crafted Ad hoc On-Demand Distance Vector (AODV) packet, which triggers an out-of-bounds memory access.	tcpdump	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2160
6950	CVE-2014-8768	Medium		Multiple Integer underflows in the geonet_print function in tcpdump 4.5.0 through 4.6.2, when in verbose mode, allow remote attackers to cause a denial of service (segmentation fault and crash) via a crafted length value in a Geonet frame.	tcpdump	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2112
6951	CVE-2014-8767	Medium		Integer underflow in the olsr_print function in tcpdump 3.9.6 through 4.6.2, when in verbose mode, allows remote attackers to cause a denial of service (crash) via a crafted length value in an OLSR frame.	tcpdump	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2145
6952	CVE-2014-8750	Medium		Race condition in the VMware driver in OpenStack Compute (Nova) before 2014.1.4 and 2014.2 before 2014.2rc1 allows remote authenticated users to access unintended consoles by spawning an instance that triggers the same VNC port to be allocated to two different instances.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2183

	A	B	C	D	E	F	G	H	I	J	K	L	M
6953	CVE-2014-8738	Medium		The _bfd_slurp_extended_name_table function in bfd/archive.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (invalid write, segmentation fault, and crash) via a crafted extended name table in an archive.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-124
6954	CVE-2014-8737	Low		Multiple directory traversal vulnerabilities in GNU binutils 2.24 and earlier allow local users to delete arbitrary files via a .. (dot dot) or full path name in an archive to (1) strip or (2) objcopy or create arbitrary files via (3) a .. (dot dot) or full path name in an archive to ar.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2439
6955	CVE-2014-8716	Low	Medium	The JPEG decoder in ImageMagick before 6.8.9-9 allows local users to cause a denial of service (out-of-bounds memory access and crash).	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4054
6956	CVE-2014-8714	Medium		The dissect_write_structured_field function in epan/dissectors/packet-tn5250.c in the TN5250 dissector in Wireshark 1.10.x before 1.10.11 and 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2099
6957	CVE-2014-8713	Medium		Stack-based buffer overflow in the build_expert_data function in epan/dissectors/packet-ncp2222.inc in the NCP dissector in Wireshark 1.10.x before 1.10.11 and 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2131
6958	CVE-2014-8712	Medium		The build_expert_data function in epan/dissectors/packet-ncp2222.inc in the NCP dissector in Wireshark 1.10.x before 1.10.11 and 1.12.x before 1.12.2 does not properly initialize a data structure, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2156
6959	CVE-2014-8711	Medium		Multiple integer overflows in epan/dissectors/packet-amqp.c in the AMQP dissector in Wireshark 1.10.x before 1.10.11 and 1.12.x before 1.12.2 allow remote attackers to cause a denial of service (application crash) via a crafted amqp_0_10 PDU in a packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2101
6960	CVE-2014-8710	Medium		The decompress_sigcomp_message function in epan/sigcomp-udvm.c in the SigComp UDVM dissector in Wireshark 1.10.x before 1.10.11 allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted packet.	wireshark	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2114
6961	CVE-2014-8709	Medium		The ieee80211_fragment function in net/mac80211/tx.c in the Linux kernel before 3.13.5 does not properly maintain a certain tail pointer, which allows remote attackers to obtain sensitive cleartext information by reading packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2132
6962	CVE-2014-8680	Medium		The GeoIP functionality in ISC BIND 9.10.0 through 9.10.1 allows remote attackers to cause a denial of service (assertion failure and named exit) via vectors related to (1) the lack of GeoIP databases for both IPv4 and IPv6, or (2) IPv6 support with certain options.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2422
6963	CVE-2014-8628	High		Memory leak in PolarSSL before 1.2.12 and 1.3.x before 1.3.9 allows remote attackers to cause a denial of service (memory consumption) via a large number of crafted X.509 certificates. NOTE: this identifier has been SPLIT per ADT3 due to different affected versions. See CVE-2014-9744 for the ClientHello message issue.	polarssl	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-775
6964	CVE-2014-8627	Medium		PolarSSL 1.3.8 does not properly negotiate the signature algorithm to use, which allows remote attackers to conduct downgrade attacks via unspecified vectors.	polarssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-791
6965	CVE-2014-8626	High		Stack-based buffer overflow in the date_from_ISO8601 function in ext/xmlrpc/libxmlrpc/xmlrpc.c in PHP before 5.2.7 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by including a timezone field in a date, leading to improper XML-RPC encoding.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2107
6966	CVE-2014-8625	Medium		Multiple format string vulnerabilities in the parse_error_msg function in parsehelp.c in dpkg before 1.17.22 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via format string specifiers in the (1) package or (2) architecture name.	dpkg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-133
6967	CVE-2014-8595	Low		arch/x86/x86_emulate/x86_emulate.c in Xen 3.2.1 through 4.4.x does not properly check privileges, which allows local HVM guest users to gain privileges or cause a denial of service (crash) via a crafted (1) CALL, (2) JMP, (3) RETF, (4) LCALL, (5) LJMP, or (6) LRET far branch instruction.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2243
6968	CVE-2014-8594	Medium		The do_mmu_update function in arch/x86/mm.c in Xen 4.x through 4.4.x does not properly restrict updates to only PV page tables, which allows remote PV guests to cause a denial of service (NULL pointer derference) by leveraging hardware emulation services for HVM guests using Hardware Assisted Paging (HAP).	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2229
6969	CVE-2014-8564	Medium		The _gnutls_ecc_ansi_x963_export function in gnutls_ecc.c in GnuTLS 3.x before 3.1.28, 3.2.x before 3.2.20, and 3.3.x before 3.3.10 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted (1) Elliptic Curve Cryptography (ECC) certificate or (2) certificate signing requests (CSR), related to generating key IDs.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2141
6970	CVE-2014-8559	Medium		The d_walk function in fs/dcache.c in the Linux kernel through 3.17.2 does not properly maintain the semantics of rename_lock, which allows local users to cause a denial of service (deadlock and system hang) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2115
6971	CVE-2014-8549	High		libavcodec/on2avc.c in FFmpeg before 2.4.2 does not constrain the number of channels to at most 2, which allows remote attackers to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via crafted On2 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2164

	A	B	C	D	E	F	G	H	I	J	K	L	M
6972	CVE-2014-8548	High		Off-by-one error in libavcodec/smc.c in FFmpeg before 2.4.2 allows remote attackers to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via crafted Quicktime Graphics (aka SMC) video data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8736
6973	CVE-2014-8547	High		libavcodec/gifdec.c in FFmpeg before 2.4.2 does not properly compute image heights, which allows remote attackers to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via crafted GIF data.	ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2105
6974	CVE-2014-8546	High		Integer underflow in libavcodec/cinepak.c in FFmpeg before 2.4.2 allows remote attackers to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via crafted Cinepak video data.	ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2138
6975	CVE-2014-8545	High		libavcodec/pngdec.c in FFmpeg before 2.4.2 accepts the monochrome-black format without verifying that the bits-per-pixel value is 1, which allows remote attackers to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via crafted PNG data.	ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2110
6976	CVE-2014-8544	High		libavcodec/tiff.c in FFmpeg before 2.4.2 does not properly validate bits-per-pixel fields, which allows remote attackers to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via crafted TIFF data.	ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2144
6977	CVE-2014-8543	High		libavcodec/mmvideo.c in FFmpeg before 2.4.2 does not consider all lines of HHV intra blocks during validation of image height, which allows remote attackers to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via crafted MM video data.	ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2130
6978	CVE-2014-8542	High		libavcodec/utils.c in FFmpeg before 2.4.2 omits a certain codec ID during enforcement of alignment, which allows remote attackers to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via crafted JV data.	ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2161
6979	CVE-2014-8541	High		libavcodec/mjpegdec.c in FFmpeg before 2.4.2 considers only dimension differences, and not bits-per-pixel differences, when determining whether an image size has changed, which allows remote attackers to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via crafted MJPEG data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8752
6980	CVE-2014-8504	High		Stack-based buffer overflow in the srec_scan function in bfd/srec.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (crash) and possibly have other unspecified impact via a crafted file.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2435
6981	CVE-2014-8503	High		Stack-based buffer overflow in the ihex_scan function in bfd/ihex.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (crash) and possibly have other unspecified impact via a crafted ihex file.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2407
6982	CVE-2014-8502	High		Heap-based buffer overflow in the pe_print_edata function in bfd/peXXigen.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (crash) and possibly have other unspecified impact via a truncated export table in a PE file.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2445
6983	CVE-2014-8501	High		The _bfd_XXi_swap_aouthdr_in function in bfd/peXXigen.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) and possibly have other unspecified impact via a crafted NumberOfRvaAndSizes field in the AOUT header in a PE executable.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2423
6984	CVE-2014-8500	High		ISC BIND 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1 does not limit delegation chaining, which allows remote attackers to cause a denial of service (memory consumption and named crash) via a large or infinite number of referrals.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2416
6985	CVE-2014-8485	High		The setup_group function in bfd/elf.c in libbfd in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted section group headers in an ELF file.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2440
6986	CVE-2014-8484	Medium		The srec_scan function in bfd/srec.c in libdbfd in GNU binutils before 2.25 allows remote attackers to cause a denial of service (out-of-bounds read) via a small S-record.	binutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2427
6987	CVE-2014-8481	Medium		The instruction decoder in arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel before 3.18-rc2 does not properly handle invalid instructions, which allows guest OS users to cause a denial of service (NULL pointer dereference and host OS crash) via a crafted application that triggers (1) an improperly fetched instruction or (2) an instruction that occupies too many bytes. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8480.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2118
6988	CVE-2014-8480	Medium		The instruction decoder in arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel before 3.18-rc2 lacks intended decoder-table flags for certain RIP-relative instructions, which allows guest OS users to cause a denial of service (NULL pointer dereference and host OS crash) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2168
6989	CVE-2014-8369	Medium		The kvm_iommu_map_pages function in virt/kvm/iommu.c in the Linux kernel through 3.17.2 miscalculates the number of pages during the handling of a mapping failure, which allows guest OS users to cause a denial of service (host OS page unpinning) or possibly have unspecified other impact by leveraging guest OS privileges. NOTE: this vulnerability exists because of an incorrect fix for CVE-2014-3601.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8737
6990	CVE-2014-8355	Medium	Medium	PCX parser code in ImageMagick before 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds read).	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4059

	A	B	C	D	E	F	G	H	I	J	K	L	M
6991	CVE-2014-8354	Medium	Medium	The HorizontalFilter function in resize.c in ImageMagick before 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image file.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4080
6992	CVE-2014-8326	Low		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.5, 4.1.x before 4.1.14.6, and 4.2.x before 4.2.10.1 allow remote authenticated users to inject arbitrary web script or HTML via a crafted (1) database name or (2) table name, related to the libraries/DatabaseInterface.class.php code for SQL debug output and the js/server_status_monitor.js code for the server monitor page.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2097
6993	CVE-2014-8324			network.c in Aircrack-ng before 1.2 Beta 3 allows remote attackers to cause a denial of service (segmentation fault) via a response with a crafted length parameter.	aircrack-ng	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5724
6994	CVE-2014-8323			buddy-ng.c in Aircrack-ng before 1.2 Beta 3 allows remote attackers to cause a denial of service (segmentation fault) via a response with a crafted length parameter.	aircrack-ng	Unchanged	Won't Fix	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5686
6995	CVE-2014-8322	HIGH	CRITICAL	Stack-based buffer overflow in the tcp_test function in aireplay-ng.c in Aircrack-ng before 1.2 RC 1 allows remote attackers to execute arbitrary code via a crafted length parameter value.	aircrack-ng	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3990
6996	CVE-2014-8321	MEDIUM	HIGH	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	aircrack-ng	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1019-3989
6997	CVE-2014-8275	Medium		OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-82
6998	CVE-2014-8242	MEDIUM		Michael Samuel discovered that rsync was vulnerable to checksum collisions. This could prevent rsync from running and syncing files successfully, which could break various applications that use and rely on rsync.	rsync	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-353
6999	CVE-2014-8176	HIGH		The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-450
7000	CVE-2014-8173	High		The pmd_none_or_trans_huge_or_clear_bad function in include/asm-generic/pgtable.h in the Linux kernel before 3.13 on NUMA systems does not properly determine whether a Page Middle Directory (PMD) entry is a transparent huge-table entry, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted MADV_WILLNEED madvise system call that leverages the absence of a page-table lock.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-250
7001	CVE-2014-8172	Medium		The filesystem implementation in the Linux kernel before 3.13 performs certain operations on lists of files with an inappropriate locking approach, which allows local users to cause a denial of service (soft lockup or system crash) via unspecified use of Asynchronous I/O (AIO) operations.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-239
7002	CVE-2014-8171			On a system with memory-constrained cgroups, it is possible for a non-root user to lock up the system by continuously spawning new processes within a cgroup which is already in an OOM event.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-509
7003	CVE-2014-8166			The browsing feature in the server in CUPS does not filter ANSI escape sequences from shared printer names, which might allow remote attackers to execute arbitrary code via a crafted printer name.	cups	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3057
7004	CVE-2014-8161	MEDIUM	MEDIUM	PostgreSQL before 9.0.19, 9.1.x before 9.1.15, 9.2.x before 9.2.10, 9.3.x before 9.3.6, and 9.4.x before 9.4.1 allows remote authenticated users to obtain sensitive column values by triggering constraint violation and then reading the error message.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1019-3992
7005	CVE-2014-8160	Medium		net/netfilter/nf_conntrack_proto_generic.c in the Linux kernel before 3.18 generates incorrect conntrack entries during handling of certain iptables rule sets for the SCTP, DCCP, GRE, and UDP-Lite protocols, which allows remote attackers to bypass intended access restrictions via packets with disallowed port numbers.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-220
7006	CVE-2014-8159	Medium		The InfiniBand (IB) implementation in the Linux kernel package before 2.6.32-504.12.2 on Red Hat Enterprise Linux (RHEL) 6 does not properly restrict use of User Verbs for registration of memory regions, which allows local users to access arbitrary physical memory locations, and consequently cause a denial of service (system crash) or gain privileges, by leveraging permissions on a uverbs device under /dev/infiniband/.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-235
7007	CVE-2014-8158	Medium		Multiple stack-based buffer overflows in jpc_qmfb.c in JasPer 1.900.1 and earlier allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted JPEG 2000 image.	jasper	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-456
7008	CVE-2014-8157	High		Off-by-one error in the jpc_dec_process_sot function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted JPEG 2000 image, which triggers a heap-based buffer overflow.	jasper	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-455

	A	B	C	D	E	F	G	H	I	J	K	L	M
7009	CVE-2014-8156			The D-Bus security policy files in /etc/dbus-1/system.d/*.conf in fso-gsmd 0.12.0-3, fso-frameworkd 0.9.5.9+git20110512-4, and fso-usaged 0.12.0-2 as packaged in Debian, the upstream cornucopia.git (fsoaudiod, fsodatad, fsodeviced, fsogsmd, fsonetworkd, fsotdld, fsousaged) git master on 2015-01-19, the upstream framework.git 0.10.1 and git master on 2015-01-19, phonefsod 0.1+git20121018-1 as packaged in Debian, Ubuntu and potentially other packages, and potentially other fso modules do not properly filter D-Bus message paths, which might allow local users to cause a denial of service (dbus-daemon memory consumption), or execute arbitrary code as root by sending a crafted D-Bus message to any D-Bus system service.	dbus	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5447
7010	CVE-2014-8155	MEDIUM		It was found that gnutls, did not perform date/time check on CA certificates. Applications compiled against gnutls, will continue to assume that a certificate is valid, even though the CA certificate, (which signed this certificate) has expired.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-604
7011	CVE-2014-8154	High		The Gst.MapInfo function in Vala 0.26.0 and 0.26.1 uses an incorrect buffer length declaration for the Gstreamer bindings, which allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via unspecified vectors, which trigger a heap-based buffer overflow.	vala	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-139
7012	CVE-2014-8151	Medium		The darwinssl_connect_step1 function in lib/vtls/curl_darwinssl.c in libcurl 7.31.0 through 7.39.0, when using the DarwinSSL (aka SecureTransport) back-end for TLS, does not check if a cached TLS session validated the certificate when reusing the session, which allows man-in-the-middle attackers to spoof servers via a crafted certificate.CWE-295: Improper Certificate Validation	libcurl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-127
7013	CVE-2014-8150	Medium		CRLF injection vulnerability in libcurl 6.0 through 7.x before 7.40.0, when using an HTTP proxy, allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via CRLF sequences in a URL.CWE-93: CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection')	libcurl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-141
7014	CVE-2014-8147	HIGH		An integer overflow was found in ICU's resolveImplicitLevels function. The overflow causes an error when performing a malloc on pBiDi->insertPoints->points because insertPoints is adjacent in memory to isolates[].	icu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-360
7015	CVE-2014-8146	HIGH		A heap overflow was found in ICU's isolateCount which, under certain circumstances, is incremented too many times, resulting in several out of bounds writes.	icu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-361
7016	CVE-2014-8143	High		Samba 4.0.x before 4.0.24, 4.1.x before 4.1.16, and 4.2.x before 4.2rc4, when an Active Directory Domain Controller (AD DC) is configured, allows remote authenticated users to set the LDB userAccountControl UF_SERVER_TRUST_ACCOUNT bit, and consequently gain privileges, by leveraging delegation of authority for user-account or computer-account creation.	samba	Unchanged	8.0.0.2	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-112
7017	CVE-2014-8142	High		Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.36, 5.5.x before 5.5.20, and 5.6.x before 5.6.4 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate keys within the serialized properties of an object, a different vulnerability than CVE-2004-1019.CWE-416: Use After Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2564
7018	CVE-2014-8141			The read errors show problems in process.c:getZip64Data(), which lacked any error detection or reporting, and was trying to extract multi-byte data from a buffer which did not contain enough bytes.	unzip	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-459
7019	CVE-2014-8140			The write error shows a problem in extract.c:test_compr_eb(), which was not expecting an uncompressed size of zero for an EF_NTSD extra block.	unzip	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-460
7020	CVE-2014-8139			The problem was an unrealistic/invalid value in a .ZIP Extra Field. There was a check (in extract.c:TestExtraField()) for an extra-block length that was too large, but no check for a too-small value. In this example, the length (ebLen) was 1, and when "(ebLen-4)" was passed to crc32(), bad things Happened	unzip	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-461
7021	CVE-2014-8138	High		Heap-based buffer overflow in the jp2_decode function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted JPEG 2000 file.	jasper	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-454
7022	CVE-2014-8137	Medium		Double free vulnerability in the jas_iccattrval_destroy function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted ICC color profile in a JPEG 2000 image file.CWE-415: Double Free	jasper	Unchanged	8.0.0.5	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-451
7023	CVE-2014-8136	Low		The (1) qemuDomainMigratePerform and (2) qemuDomainMigrateFinish2 functions in qemu/qemu_driver.c in libvirt do not unlock the domain when an ACL check fails, which allow local users to cause a denial of service via unspecified vectors.	libvirt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2559
7024	CVE-2014-8135	Low		The storageVolUpload function in storage/storage_driver.c in libvirt does not check a certain return value, which allows local users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted offset value in a virsh vol-upload command.CWE-476: NULL Pointer Dereference	libvirt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2579

	A	B	C	D	E	F	G	H	I	J	K	L	M
7025	CVE-2014-8134	LOW		The paravirt_ops_setup function in arch/x86/kernel/kvm.c in the Linux kernel through 3.18 uses an improper paravirt_enabled setting for KVM guest kernels, which makes it easier for guest OS users to bypass the ASLR protection mechanism via a crafted application that reads a 16-bit value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2434
7026	CVE-2014-8133	Low		arch/x86/kernel/tls.c in the Thread Local Storage (TLS) implementation in the Linux kernel through 3.18.1 allows local users to bypass the espfix protection mechanism, and consequently makes it easier for local users to bypass the ASLR protection mechanism, via a crafted application that makes a set_thread_area system call and later reads a 16-bit value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2558
7027	CVE-2014-8131	Medium		The qemu implementation of virConnectGetAllDomainStats in libvirt before 1.2.11 does not properly handle locks when a domain is skipped due to ACL restrictions, which allows a remote authenticated users to cause a denial of service (deadlock or segmentation fault and crash) via a request to access the users does not have privileges to access.	libvirt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-90
7028	CVE-2014-8130			The _TIFFmalloc function in tif_unix.c in LibTIFF 4.0.3 does not reject a zero size, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted TIFF image that is mishandled by the TIFFWriteScanline function in tif_write.c, as demonstrated by tiffdither.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3520
7029	CVE-2014-8129			Out-of-bounds read/write was reported in tiff2pdf libtiff tool	tiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-274
7030	CVE-2014-8128			Multiple out-of-bounds reads were reported in various libtiff tools	tiff	Unchanged	8.0.0.19	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-273
7031	CVE-2014-8127			Multiple out-of-bounds reads were reported in various libtiff tools	tiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-272
7032	CVE-2014-8124	MEDIUM		OpenStack Dashboard (Horizon) before 2014.1.3 and 2014.2.x before 2014.2.1 does not properly handle session records when using a db or memcached session engine, which allows remote attackers to cause a denial of service via a large number of requests to the login page.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2269
7033	CVE-2014-8121	MEDIUM		DB_LOOKUP in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) 2.21 and earlier does not properly check if a file is open, which allows remote attackers to cause a denial of service (infinite loop) by performing a look-up while the database is iterated over the database, which triggers the file pointer to be reset.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-242
7034	CVE-2014-8119			The find_ifcfg_path function in netcf before 0.2.7 might allow attackers to cause a denial of service (application crash) via vectors involving augeas path expressions.	netcf	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3084
7035	CVE-2014-8118	High		Integer overflow in RPM 4.12 and earlier allows remote attackers to execute arbitrary code via a crafted CPIO header in the payload section of an RPM file, which triggers a stack-based buffer overflow.	rpm	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2580
7036	CVE-2014-8117	Medium		softmagic.c in file before 5.21 does not properly limit recursion, which allows remote attackers to cause a denial of service (CPU consumption or crash) via unspecified vectors.	file	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2560
7037	CVE-2014-8116	Medium		The ELF parser (readelf.c) in file before 5.21 allows remote attackers to cause a denial of service (CPU consumption or crash) via a large number of (1) program or (2) section headers or (3) invalid capabilities.	file	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2561
7038	CVE-2014-8109	MEDIUM		mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.	apache	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2578
7039	CVE-2014-8108	Medium		The mod_dav_svn Apache HTTPD server module in Apache Subversion 1.7.x before 1.7.19 and 1.8.x before 1.8.11 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a request for a URI that triggers a lookup for a virtual transaction name that does not exist.CWE-476: NULL Pointer Dereference	subversion	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2581
7040	CVE-2014-8106	Medium		Heap-based buffer overflow in the Cirrus VGA emulator (hw/display/cirrus_vga.c) in QEMU before 2.2.0 allows local guest users to execute arbitrary code via vectors related to blit regions. NOTE: this vulnerability exists because an incomplete fix for CVE-2007-1320.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2436
7041	CVE-2014-8104	Medium		OpenVPN 2.x before 2.0.11, 2.1.x, 2.2.x before 2.2.3, and 2.3.x before 2.3.6 allows remote authenticated users to cause a denial of service (server crash) via a small control channel packet.	openvpn	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2421
7042	CVE-2014-8103	Medium		X.Org Server (aka xserver and xorg-server) 1.15.0 through 1.16.x before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) sproc_dri3_query_version, (2) sproc_dri3_open, (3) sproc_dri3_pixmap_from_buffer, (4) sproc_dri3_buffer_from_pixmap, (5) sproc_dri3_fence_from_fd, (6) sproc_dri3_fd_from_fence, (7) proc_present_query_capabilities, (8) sproc_present_query_version, (9) sproc_present_pixmap, (10) sproc_present_notify_msc, (11) sproc_present_select_input, or (12) sproc_present_query_capabilities function in the (a) DRI3 or (b) Present extension.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2426

	A	B	C	D	E	F	G	H	I	J	K	L	M
7043	CVE-2014-8102	Medium		The SProcXFixesSelectSelectionInput function in the XFixes extension in X.Org X Window System (aka X11 or X) X11R6.8.0 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length value.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2430
7044	CVE-2014-8101	Medium		The RandR extension in XFree86 4.2.0, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) SProcRRQueryVersion, (2) SProcRRGetScreenInfo, (3) SProcRRSelectInput, or (4) SProcRRConfigureOutputProperty function.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2425
7045	CVE-2014-8100	Medium		The Render extension in XFree86 4.0.1, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) ProcRenderQueryVersion, (2) SProcRenderQueryVersion, (3) SProcRenderQueryPictFormats, (4) SProcRenderQueryPictIndexValues, (5) SProcRenderCreatePicture, (6) SProcRenderChangePicture, (7) SProcRenderSetPictureClipRectangles, (8) SProcRenderFreePicture, (9) SProcRenderComposite, (10) SProcRenderScale, (11) SProcRenderCreateGlyphSet, (12) SProcRenderReferenceGlyphSet, (13) SProcRenderFreeGlyphSet, (14) SProcRenderFreeGlyphs, or (15) SProcRenderCompositeGlyphs function.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2406
7046	CVE-2014-8099	Medium		The XVideo extension in XFree86 4.0.0, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) SProcXvQueryExtension, (2) SProcXvQueryAdaptors, (3) SProcXvQueryEncodings, (4) SProcXvGrabPort, (5) SProcXvUngrabPort, (6) SProcXvPutVideo, (7) SProcXvPutStill, (8) SProcXvGetVideo, (9) SProcXvGetStill, (10) SProcXvPutImage, (11) SProcXvShmPutImage, (12) SProcXvSelectVideoNotify, (13) SProcXvSelectPortNotify, (14) SProcXvStopVideo, (15) SProcXvSetPortAttribute, (16) SProcXvGetPortAttribute, (17) SProcXvQueryBestSize, (18) SProcXvQueryPortAttributes, (19) SProcXvQueryImageAttributes, or (20) SProcXvListImageFormats function.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2412
7047	CVE-2014-8098	Medium		The GLX extension in XFree86 4.0, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) __glXDisp_Render, (2) __glXDisp_RenderLarge, (3) __glXDispSwap_VendorPrivate, (4) __glXDispSwap_VendorPrivateWithReply, (5) set_client_info, (6) __glXDispSwap_SetClientInfoARB, (7) DoSwapInterval, (8) DoGetProgramString, (9) DoGetString, (10) __glXDispSwap_RenderMode, (11) __glXDisp_GetCompressedTexImage, (12) __glXDispSwap_GetCompressedTexImage, (13) __glXDisp_FeedbackBuffer, (14) __glXDispSwap_FeedbackBuffer, (15) __glXDisp_SelectBuffer, (16) __glXDispSwap_SelectBuffer, (17) __glXDisp_Flush, (18) __glXDispSwap_Flush, (19) __glXDisp_Finish, (20) __glXDispSwap_Finish, (21) __glXDisp_ReadPixels, (22) __glXDispSwap_ReadPixels, (23) __glXDisp_GetTexImage, (24) __glXDispSwap_GetTexImage, (25) __glXDisp_GetPolygonStipple, (26) __glXDispSwap_GetPolygonStipple, (27) __glXDisp_GetSeparableFilter, (28) __glXDisp_GetSeparableFilterEXT, (29) __glXDisp_GetConvolutionFilter, (30) __glXDisp_GetConvolutionFilterEXT, (31) __glXDisp_GetHistogram, (32) __glXDisp_GetHistogramEXT, (33) __glXDisp_GetMinmax, (34) __glXDisp_GetMinmaxEXT, (35) __glXDisp_GetColorTable, (36) __glXDisp_GetColorTableSGI, (37) GetSeparableFilter, (38) GetConvolutionFilter, (39) GetHistogram, (40) GetMinmax, or (41) GetColorTable function.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2431
7048	CVE-2014-8097	Medium		The DBE extension in X.Org X Window System (aka X11 or X) X11R6.1 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) ProcDbeSwapBuffers or (2) SProcDbeSwapBuffers function.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2447
7049	CVE-2014-8096	Medium		The SProcXCMiscGetXIDList function in the XC-MISC extension in X.Org X Window System (aka X11 or X) X11R6.0 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2417

	A	B	C	D	E	F	G	H	I	J	K	L	M
7050	CVE-2014-8095	Medium		The XInput extension in X.Org X Window System (aka X11 or X) X11R4 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) SProcXChangeDeviceControl, (2) ProcXChangeDeviceControl, (3) ProcXChangeFeedbackControl, (4) ProcXSendExtensionEvent, (5) SProcXIAllowEvents, (6) SProcXIChangeCursor, (7) ProcXIChangeHierarchy, (8) SProcXIGetClientPointer, (9) SProcXIGrabDevice, (10) SProcXIUngrabDevice, (11) ProcXIUngrabDevice, (12) SProcXIPassiveGrabDevice, (13) ProcXIPassiveGrabDevice, (14) SProcXIPassiveUngrabDevice, (15) ProcXIPassiveUngrabDevice, (16) SProcXListDeviceProperties, (17) SProcXDeleteDeviceProperty, (18) SProcXIListProperties, (19) SProcXIDeleteProperty, (20) SProcXIGetProperty, (21) SProcXIQueryDevice, (22) SProcXIQueryPointer, (23) SProcXISelectEvents, (24) SProcXISetClientPointer, (25) SProcXISetFocus, (26) SProcXIGetFocus, or (27) SProcXIWarpPointer function.	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2428
7051	CVE-2014-8094	Medium		Integer overflow in the ProcDRI2GetBuffers function in the DRI2 extension in X.Org Server (aka xserver and xorg-server) 1.7.0 through 1.16.x before 1.16.3 allows remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via a crafted request, which triggers an out-of-bounds read or write.CWE-190: Integer Overflow or Wraparound	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2408
7052	CVE-2014-8093	Medium		Multiple integer overflows in the GLX extension in XFree86 4.0, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before 1.16.3 allow remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via a crafted request to the (1) __glXDisp_ReadPixels, (2) __glXDispSwap_ReadPixels, (3) __glXDisp_GetTexImage, (4) __glXDispSwap_GetTexImage, (5) GetSeparableFilter, (6) GetConvolutionFilter, (7) GetHistogram, (8) GetMinmax, (9) GetColorTable, (10) __glXGetAnswerBuffer, (11) __GLX_GET_ANSWER_BUFFER, (12) __glXMap1dReqSize, (13) __glXMap1fReqSize, (14) Map2Size, (15) __glXMap2dReqSize, (16) __glXMap2fReqSize, (17) __glXImageSize, or (18) __glXSeparableFilter2DReqSize function, which triggers an out-of-bounds read or write.CWE-190: Integer Overflow or Wraparound	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2438
7053	CVE-2014-8092	Medium		Multiple integer overflows in X.Org X Window System (aka X11 or X) X11R1 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allow remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via a crafted request to the (1) ProcPutImage, (2) GetHosts, (3) RegionSizeof, or (4) REQUEST_FIXED_SIZE function, which triggers an out-of-bounds read or write.CWE-190: Integer Overflow or Wraparound	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2424
7054	CVE-2014-8091	Medium		X.Org X Window System (aka X11 and X) X11R5 and X.Org Server (aka xserver and xorg-server) before 1.16.3, when using SUN-DES-1 (Secure RPC) authentication credentials, does not check the return value of a malloc call, which allows remote attackers to cause a denial of service (NULL pointer dereference and server crash) via a crafted connection request.CWE-476: NULL Pointer Dereference	xorg-server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2442
7055	CVE-2014-8090	Medium		The REXML parser in Ruby 1.9.x before 1.9.3 patchlevel 551, 2.0.x before 2.0.0 patchlevel 598, and 2.1.x before 2.1.5 allows remote attackers to cause a denial of service (CPU and memory consumption) a crafted XML document containing an empty string in an entity that is used in a large number of nested entity references, aka an XML Entity Expansion (XEE) attack. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-1821 and CVE-2014-8080.CWE-611: Improper Restriction of XML External Entity Reference ('XXE')	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2146
7056	CVE-2014-8086	Medium		Race condition in the ext4_file_write_iter function in fs/ext4/file.c in the Linux kernel through 3.17 allows local users to cause a denial of service (file unavailability) via a combination of a write action and an F_SETFL fcntl operation for the O_DIRECT flag.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8647
7057	CVE-2014-8080	Medium		The REXML parser in Ruby 1.9.x before 1.9.3-p550, 2.0.x before 2.0.0-p594, and 2.1.x before 2.1.4 allows remote attackers to cause a denial of service (memory consumption) via a crafted XML document, aka an XML Entity Expansion (XEE) attack.CWE-611: Improper Restriction of XML External Entity Reference ('XXE')	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2121

	A	B	C	D	E	F	G	H	I	J	K	L	M
7058	CVE-2014-7975	Medium		The do_umount function in fs/namespace.c in the Linux kernel through 3.17 does not require the CAP_SYS_ADMIN capability for do_remount_sb calls that change the root filesystem to read-only, which allows local users to cause a denial of service (loss of writability) by making certain unshare system calls, clearing the / MNT_LOCKED flag, and making an MNT_FORCE umount system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8673
7059	CVE-2014-7970	Medium		The pivot_root implementation in fs/namespace.c in the Linux kernel through 3.17 does not properly interact with certain locations of a chroot directory, which allows local users to cause a denial of service (mount-tree loop) via . (dot) values in both arguments to the pivot_root system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8661
7060	CVE-2014-7960	Medium		OpenStack Object Storage (Swift) before 2.2.0 allows remote authenticated users to bypass the max_meta_count and other metadata constraints via multiple crafted requests which exceed the limit when combined.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2184
7061	CVE-2014-7937	High		Multiple off-by-one errors in libavcodec/vorbisdec.c in FFmpeg before 2.4.2, as used in Google Chrome before 40.0.2214.91, allow remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Vorbis I data.	gst-ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-130
7062	CVE-2014-7933	High		Use-after-free vulnerability in the matroska_read_seek function in libavformat/matroskadec.c in FFmpeg before 2.5.1, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Matroska file that triggers improper maintenance of tracks data.CWE-416: Use After Free	gst-ffmpeg	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-111
7063	CVE-2014-7853	Medium		The JBoss Application Server (WildFly) JacORB subsystem in Red Hat JBoss Enterprise Application Platform (EAP) before 6.3.3 does not properly assign socket-binding-ref sensitivity classification to the security-domain attribute, which allows remote authenticated users to obtain sensitive information by leveraging access to the security-domain attribute.	jboss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2319
7064	CVE-2014-7843	MEDIUM		The __clear_user function in arch/arm64/lib/clear_user.S in the Linux kernel before 3.17.4 on the ARM64 platform allows local users to cause a denial of service (system crash) by reading one byte beyond a /dev/zero page boundary.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2148
7065	CVE-2014-7842	MEDIUM		Race condition in arch/x86/kvm/x86.c in the Linux kernel before 3.17.4 allows guest OS users to cause a denial of service (guest OS crash) via a crafted application that performs an MMIO transaction or a PIO transaction to trigger a guest userspace emulation error report, a similar issue to CVE-2010-5313.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2150
7066	CVE-2014-7841	MEDIUM		The sctp_process_param function in net/sctp/sm_make_chunk.c in the SCTP implementation in the Linux kernel before 3.17.4, when ASCONF is used, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via a malformed INIT chunk.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2158
7067	CVE-2014-7840	HIGH		The host_from_stream_offset function in arch_init.c in QEMU, when loading RAM during migration, allows remote attackers to execute arbitrary code via a crafted (1) offset or (2) length value in savevm data.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2420
7068	CVE-2014-7826	Medium		kernel/trace/trace_syscalls.c in the Linux kernel through 3.17.2 does not properly handle private syscall numbers during use of the ftrace subsystem, which allows local users to gain privileges or cause a denial of service (invalid pointer dereference) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2117
7069	CVE-2014-7825	Medium		kernel/trace/trace_syscalls.c in the Linux kernel through 3.17.2 does not properly handle private syscall numbers during use of the perf subsystem, which allows local users to cause a denial of service (out-of-bounds read and OOPS) or bypass the ASLR protection mechanism via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2169
7070	CVE-2014-7824	Low		D-Bus 1.3.0 through 1.6.x before 1.6.26, 1.8.x before 1.8.10, and 1.9.x before 1.9.2 allows local users to cause a denial of service (prevention of new connections and connection drop) by queuing the maximum number of file descriptors. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-3636.1.	dbus	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2104
7071	CVE-2014-7823	Medium		The virDomainGetXMLDesc API in Libvirt before 1.2.11 allows remote read-only users to obtain the VNC password by using the VIR_DOMAIN_XML_MIGRATABLE, which triggers the use of the VIR_DOMAIN_XML_SECURE flag.	libvirt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2151
7072	CVE-2014-7822	High		The implementation of certain splice_write file operations in the Linux kernel before 3.16 does not enforce a restriction on the maximum size of a single file, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted splice system call, as demonstrated by use of a file descriptor associated with an ext4 filesystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-241
7073	CVE-2014-7821	Medium		OpenStack Neutron before 2014.1.4 and 2014.2.x before 2014.2.1 allows remote authenticated users to cause a denial of service (crash) via a crafted dns_nameservers value in the DNS configuration.	openstack neutron	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2255
7074	CVE-2014-7817	Medium		The wordexp function in GNU C Library (aka glibc) 2.21 does not enforce the WRDE_NOCMD flag, which allows context-dependent attackers to execute arbitrary commands, as demonstrated by input containing $((`...`)).	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2147

	A	B	C	D	E	F	G	H	I	J	K	L	M
7075	CVE-2014-7815	Medium		The set_pixel_format function in ui/vnc.c in QEMU allows remote attackers to cause a denial of service (crash) via a small bytes_per_pixel value.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2124
7076	CVE-2014-7284	Medium		The net_get_random_once implementation in net/core/utils.c in the Linux kernel 3.13.x and 3.14.x before 3.14.5 on certain Intel processors does not perform the intended slow-path operation to initialize random seeds, which makes it easier for remote attackers to spoof or disrupt IP communication by leveraging the predictability of TCP sequence numbers, TCP and UDP port numbers, and IP ID values.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8663
7077	CVE-2014-7283	Medium		The xfs_da3_fixhashpath function in fs/xfs/xfs_da_btree.c in the xfs implementation in the Linux kernel before 3.14.2 does not properly compare btree hash values, which allows local users to cause a denial of service (filesystem corruption, and OOPS or panic) via operations on directories that have hash collisions, as demonstrated by rmdir operations.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8649
7078	CVE-2014-7231	Low		The strutils.mask_password function in the OpenStack Oslo utility library, Cinder, Nova, and Trove before 2013.2.4 and 2014.1 before 2014.1.3 does not properly mask passwords when logging commands, which allows local users to obtain passwords by reading the log.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2154
7079	CVE-2014-7230	Low		The processutils.execute function in OpenStack oslo-incubator, Cinder, Nova, and Trove before 2013.2.4 and 2014.1 before 2014.1.3 allows local users to obtain passwords from commands that cause a ProcessExecutionError by reading the log.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2164
7080	CVE-2014-7217	Low		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.4, 4.1.x before 4.1.14.5, and 4.2.x before 4.2.9.1 allow remote authenticated users to inject arbitrary web script or HTML via a crafted ENUM value that is improperly handled during rendering of the (1) table search or (2) table structure page, related to libraries/TableSearch.class.php and libraries/Util.class.php.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8558
7081	CVE-2014-7207	Medium		A certain Debian patch to the IPv6 implementation in the Linux kernel 3.2.x through 3.2.63 does not properly validate arguments in ipv6_select_ident function calls, which allows local users to cause a denial of service (NULL pointer dereference and system crash) by leveraging (1) tun or (2) macvtap device access.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2167
7082	CVE-2014-7188	High		The hvm_msr_read_intercept function in arch/x86/hvm/hvm.c in Xen 4.1 through 4.4.x uses an improper MSR range for x2APIC emulation, which allows local HVM guests to cause a denial of service (host crash) or read data from the hypervisor or other guests via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2153
7083	CVE-2014-7187	High		Off-by-one error in the read_token_word function in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via deeply nested for loops, aka the word_lineno issue.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8507
7084	CVE-2014-7186	High		The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via crafted use of here documents, aka the redir_stack issue.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8506
7085	CVE-2014-7185	Medium		Integer overflow in bufferobject.c in Python before 2.7.8 allows context-dependent attackers to obtain sensitive information from process memory via a large size and offset in a buffer function.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8555
7086	CVE-2014-7169	High		GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8505
7087	CVE-2014-7156	Low		The x86_emulate function in arch/x86/x86_emulate/x86_emulate.c in Xen 3.3.x through 4.4.x does not check the supervisor mode permissions for instructions that generate software interrupts, which allows local HVM guest users to cause a denial of service (guest crash) via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2157
7088	CVE-2014-7155	Medium		The x86_emulate function in arch/x86/x86_emulate/x86_emulate.c in Xen 4.4.x and earlier does not properly check supervisor mode permissions, which allows local HVM users to cause a denial of service (guest crash) or gain guest kernel mode privileges via vectors involving an (1) HLT, (2) LGDT, (3) LIDT, or (4) LMSW instruction.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2166
7089	CVE-2014-7154	Medium		Race condition in HVMOP_track_dirty_vram in Xen 4.0.0 through 4.4.x does not ensure possession of the guarding lock for dirty video RAM tracking, which allows certain local guest domains to cause a denial of service via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2151

	A	B	C	D	E	F	G	H	I	J	K	L	M
7090	CVE-2014-7145	High		The SMB2_tcon function in fs/cifs/smb2pdu.c in the Linux kernel before 3.16.3 allows remote CIFS servers to cause a denial of service (NULL pointer dereference and client system crash) or possibly have unspecified other impact by deleting the IPC$ share during resolution of DFS referrals.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8559
7091	CVE-2014-7144	Medium		OpenStack keystonemiddleware (formerly python-keystoneclient) 0.x before 0.11.0 and 1.x before 1.2.0 disables certification verification when the insecure option is set in a paste configuration (paste.ini) file regardless of the value, which allows remote attackers to conduct man-in-the-middle attacks via a crafted certificate.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2150
7092	CVE-2014-7142	Medium		The pinger in Squid 3.x before 3.4.8 allows remote attackers to obtain sensitive information or cause a denial of service (crash) via a crafted (1) ICMP or (2) ICMP6 packet size.	squid	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2154
7093	CVE-2014-7141	Medium		The pinger in Squid 3.x before 3.4.8 allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and crash) via a crafted type in an (1) ICMP or (2) ICMP6 packet.	squid	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2120
7094	CVE-2014-6568	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.40 and earlier, and 5.6.21 and earlier, allows remote authenticated users to affect availability via vectors related to Server : InnoDB : DML.	mysql	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-126
7095	CVE-2014-6564	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.19 and earlier allows remote authenticated users to affect availability via vectors related to SERVER:INNODB FULLTEXT SEARCH DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8670
7096	CVE-2014-6559	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier, and 5.6.20 and earlier, allows remote attackers to affect confidentiality via vectors related to C API SSL CERTIFICATE HANDLING.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8659
7097	CVE-2014-6555	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier and 5.6.20 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to SERVER:DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8650
7098	CVE-2014-6551	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier and 5.6.19 and earlier allows local users to affect confidentiality via vectors related to CLIENT:MYSQLADMIN.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8671
7099	CVE-2014-6530	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier, and 5.6.19 and earlier, allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to CLIENT:MYSQLDUMP.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8652
7100	CVE-2014-6520	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier allows remote authenticated users to affect availability via vectors related to SERVER:DDL.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8677
7101	CVE-2014-6507	High		Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier, and 5.6.20 and earlier, allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to SERVER:DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8655
7102	CVE-2014-6505	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier, and 5.6.19 and earlier, allows remote authenticated users to affect availability via vectors related to SERVER:MEMORY STORAGE ENGINE.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8660
7103	CVE-2014-6500	High		Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier, and 5.6.20 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to SERVER:SSL:yaSSL, a different vulnerability than CVE-2014-6491.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8653
7104	CVE-2014-6496	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier, and 5.6.20 and earlier, allows remote attackers to affect availability via vectors related to CLIENT:SSL:yaSSL, a different vulnerability than CVE-2014-6494.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8662
7105	CVE-2014-6495	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier, and 5.6.19 and earlier, allows remote attackers to affect availability via vectors related to SERVER:SSL:yaSSL.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8674
7106	CVE-2014-6494	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier, and 5.6.20 and earlier, allows remote attackers to affect availability via vectors related to CLIENT:SSL:yaSSL, a different vulnerability than CVE-2014-6496.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8651
7107	CVE-2014-6491	High		Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier and 5.6.20 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to SERVER:SSL:yaSSL, a different vulnerability than CVE-2014-6500.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8672
7108	CVE-2014-6489	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.19 and earlier allows remote authenticated users to affect integrity and availability via vectors related to SERVER:SP.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8669
7109	CVE-2014-6484	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier, and 5.6.19 and earlier, allows remote authenticated users to affect availability via vectors related to SERVER:DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8657
7110	CVE-2014-6478	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier, and 5.6.19 and earlier, allows remote attackers to affect integrity via vectors related to SERVER:SSL:yaSSL.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8665
7111	CVE-2014-6474	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.19 and earlier allows remote authenticated users to affect availability via vectors related to SERVER:MEMCACHED.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8675
7112	CVE-2014-6469	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier and 5.6.20 and earlier allows remote authenticated users to affect availability via vectors related to SERVER:OPTIMIZER.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8667

	A	B	C	D	E	F	G	H	I	J	K	L	M
7113	CVE-2014-6464	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier and 5.6.20 and earlier allows remote authenticated users to affect availability via vectors related to SERVER:INNODB DML FOREIGN KEYS.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8664
7114	CVE-2014-6463	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier and 5.6.19 and earlier allows remote authenticated users to affect availability via vectors related to SERVER:REPLICATION ROW FORMAT BINARY LOG DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8658
7115	CVE-2014-6438			The URI.decode_www_form_component method in Ruby before 1.9.2-p330 allows remote attackers to cause a denial of service (catastrophic regular expression backtracking, resource consumption, or application crash) via a crafted string.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5306
7116	CVE-2014-6418	High		net/ceph/auth_x.c in Ceph, as used in the Linux kernel before 3.16.3, does not properly validate auth replies, which allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via crafted data from the IP address of a Ceph Monitor.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8540
7117	CVE-2014-6417	High		net/ceph/auth_x.c in Ceph, as used in the Linux kernel before 3.16.3, does not properly consider the possibility of kmalloc failure, which allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via a long unencrypted auth ticket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8552
7118	CVE-2014-6416	High		Buffer overflow in net/ceph/auth_x.c in Ceph, as used in the Linux kernel before 3.16.3, allows remote attackers to cause a denial of service (memory corruption and panic) or possibly have unspecified other impact via a long unencrypted auth ticket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8557
7119	CVE-2014-6414	Medium		OpenStack Neutron before 2014.2.4 and 2014.1 before 2014.1.2 allows remote authenticated users to set admin network attributes to default values via unspecified vectors.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2170
7120	CVE-2014-6410	Medium		The __udf_read_inode function in fs/udf/inode.c in the Linux kernel through 3.16.3 does not restrict the amount of ICB indirection, which allows physically proximate attackers to cause a denial of service (infinite loop or stack consumption) via a UDF filesystem with a crafted inode.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8542
7121	CVE-2014-6300	Medium		Cross-site scripting (XSS) vulnerability in the micro history implementation in phpMyAdmin 4.0.x before 4.0.10.3, 4.1.x before 4.1.14.4, and 4.2.x before 4.2.8.1 allows remote attackers to inject arbitrary web script or HTML, and consequently conduct a cross-site request forgery (CSRF) attack to create a root account, via a crafted URL, related to js/ajax.js.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2119
7122	CVE-2014-6278	High		GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary commands via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271, CVE-2014-7169, and CVE-2014-6277.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8510
7123	CVE-2014-6277	High		GNU Bash through 4.3 bash43-026 does not properly parse function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access, and untrusted-pointer read and write operations) via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271 and CVE-2014-7169.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8508
7124	CVE-2014-6272	High		Multiple integer overflows in the evbuffer API in Libevent 1.4.x before 1.4.15, 2.0.x before 2.0.22, and 2.1.x before 2.1.5-beta allow context-dependent attackers to cause a denial of service or possibly have other unspecified impact via insanely large inputs to the (1) evbuffer_add, (2) evbuffer_expand, or (3) bufferevent_write function, which triggers a heap-based buffer overflow or an infinite loop. NOTE: this identifier has been SPLIT per ADT3 due to different affected versions. See CVE-2015-6525 for the functions that are only affected in 2.0 and later.	libevent	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-782
7125	CVE-2014-6271	High		GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka ShellShock. NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8504
7126	CVE-2014-6268	Medium		The evtchn_fifo_set_pending function in Xen 4.4.x allows local guest users to cause a denial of service (host crash) via vectors involving an uninitialized FIFO-based event channel control block when (1) binding or (2) moving an event to a different VCPU.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2287

	A	B	C	D	E	F	G	H	I	J	K	L	M
7127	CVE-2014-6040	Medium		GNU C Library (aka glibc) before 2.20 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via a multibyte character value of 0xffff to the iconv function when converting (1) IBM933, (2) IBM935, (3) IBM937, (4) IBM939, or (5) IBM1364 encoded data to UTF-8.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2418
7128	CVE-2014-5472	Medium		The parse_rock_ridge_inode_internal function in fs/isofs/rock.c in the Linux kernel through 3.16.1 allows local users to cause a denial of service (unkillable mount process) via a crafted iso9660 image with a self-referential CL entry.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8417
7129	CVE-2014-5471	Medium		Stack consumption vulnerability in the parse_rock_ridge_inode_internal function in fs/isofs/rock.c in the Linux kernel through 3.16.1 allows local users to cause a denial of service (uncontrolled recursion, and system crash or reboot) via a crafted iso9660 image with a CL entry referring to a directory entry that has a CL entry.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8418
7130	CVE-2014-5461	Medium		Buffer overflow in the vararg functions in ldo.c in Lua 5.1 through 5.2.x before 5.2.3 allows context-dependent attackers to cause a denial of service (crash) via a small number of arguments to a function with a large number of fixed arguments.	lua	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8415
7131	CVE-2014-5459	Low		The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8546
7132	CVE-2014-5455	Medium		Unquoted Windows search path vulnerability in the ptservice service in PrivateTunnel 2.3.8, as bundled in OpenVPN 2.1.28.0 allows local users to gain privileges via a crafted program.exe file in the %SYSTEMDRIVE% folder.CWE-428: Unquoted Search Path or Element	openvpn	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8280
7133	CVE-2014-5388	Medium		Off-by-one error in the pci_read function in the ACPI PCI hotplug interface (hw/acpi/pcihp.c) in QEMU allows local guest users to obtain sensitive information and have other unspecified impact related to a crafted PCI device that triggers memory corruption.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2152
7134	CVE-2014-5356	Medium		OpenStack Image Registry and Delivery Service (Glance) before 2013.2.4, 2014.x before 2014.1.3, and Juno before Juno-3, when using the V2 API, does not properly enforce the image_size_cap configuration option, which allows remote authenticated users to cause a denial of service (disk consumption) by uploading a large image.	openstack glance	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2069
7135	CVE-2014-5355	Medium		MIT Kerberos 5 (aka krb5) through 1.13.1 incorrectly expects that a krb5_read_message data field is represented as a string ending with a '\0' character, which allows remote attackers to (1) cause a denial of service (NULL pointer dereference) via a zero-byte version string or (2) cause a denial of service (out-of-bounds read) by omitting the '\0' character, related to appl/user_user/server.c and lib/krb5/krb/recvauth.c.CWE-476: NULL Pointer Dereference	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-187
7136	CVE-2014-5354	Low		plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.1, when the KDC uses LDAP, allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) by creating a database entry for a keyless principal, as demonstrated by a kadmin add_principal -nokey or purgekeys -all command.CWE-476: NULL Pointer Dereference	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2562
7137	CVE-2014-5353	Low		The krb5_ldap_get_password_policy_from_dn function in plugins/kdb/ldap/libkdb_ldap/ldap_pwd_policy.c in MIT Kerberos 5 (aka krb5) before 1.13.1, when the KDC uses LDAP, allows remote authenticated users to cause a denial of service (daemon crash) via a successful LDAP query with no results, as demonstrated by using an incorrect object type for a password policy.CWE-476: NULL Pointer Dereference	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2565
7138	CVE-2014-5352	High		The krb5_gss_process_context_token function in lib/gssapi/krb5/process_context_token.c in the libgssapi_krb5 library in MIT Kerberos 5 (aka krb5) through 1.11.5, 1.12.x through 1.12.2, and 1.13.x before 1.13.1 does not properly maintain security-context handles, which allows remote authenticated users to cause a denial of service (use-after-free and double free, and daemon crash) or possibly execute arbitrary code via crafted GSSAPI traffic, as demonstrated by traffic to kadmind.CWE-416: Use After Free	krb5	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-181
7139	CVE-2014-5351	LOW		The kadm5_randkey_principal_3 function in lib/kadm5/srv/svr_principal.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13 sends old keys in a response to a -randkey -keepold request, which allows remote authenticated users to forge tickets by leveraging administrative access.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8543
7140	CVE-2014-5332	Medium		Race condition in NVMap in NVIDIA Tegra Linux Kernel 3.10 allows local users to gain privileges via a crafted NVMAP_IOC_CREATE IOCTL call, which triggers a use-after-free error, as demonstrated by using a race condition to escape the Chrome sandbox.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-193

	A	B	C	D	E	F	G	H	I	J	K	L	M
7141	CVE-2014-5282			Docker before 1.3 does not properly validate image IDs, which allows remote attackers to redirect to another image through the loading of untrusted images via 'docker load'.	docker	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3347
7142	CVE-2014-5274	Low		Cross-site scripting (XSS) vulnerability in the view operations page in phpMyAdmin 4.1.x before 4.1.14.3 and 4.2.x before 4.2.7.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted view name, related to js/functions.js.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8275
7143	CVE-2014-5273	Low		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.0.x before 4.0.10.2, 4.1.x before 4.1.14.3, and 4.2.x before 4.2.7.1 allow remote authenticated users to inject arbitrary web script or HTML via the (1) browse table page, related to js/sql.js; (2) ENUM editor page, related to js/functions.js; (3) monitor page, related to js/server_status_monitor.js; (4) query charts page, related to js/tbl_chart.js; or (5) table relations page, related to libraries/tbl_relation.lib.php.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8276
7144	CVE-2014-5272	Medium		libavcodec/iff.c in FFMpeg before 1.1.14, 1.2.x before 1.2.8, 2.2.x before 2.2.7, and 2.3.x before 2.3.2 allows remote attackers to have unspecified impact via a crafted iff image, which triggers an out-of-bounds array access, related to the rgb8 and rgbn formats.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2125
7145	CVE-2014-5271	High		Heap-based buffer overflow in the encode_slice function in libavcodec/proresenc_kostya.c in FFMpeg before 1.1.14, 1.2.x before 1.2.8, 2.x before 2.2.7, and 2.3.x before 2.3.3 and Libav before 10.5 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via unspecified vectors.	ffmpeg & libav	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8755
7146	CVE-2014-5270	Low		Libgcrypt before 1.5.4, as used in GnuPG and other products, does not properly perform ciphertext normalization and ciphertext randomization, which makes it easier for physically proximate attackers to conduct key-extraction attacks by leveraging the ability to collect voltage data from exposed metal, a different vector than CVE-2013-4576.	libgcrypt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8544
7147	CVE-2014-5263	Medium		vmstate_xhci_event in hw/usb/hcd-xhci.c in QEMU 1.6.0 does not terminate the list with the VMSTATE_END_OF_LIST macro, which allows attackers to cause a denial of service (out-of-bounds access, infinite loop, and memory corruption) and possibly gain privileges via unspecified vectors.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8274
7148	CVE-2014-5252	Medium		The V3 API in OpenStack Identity (Keystone) 2014.1.x before 2014.1.2.1 and Juno before Juno-3 updates the issued_at value for UUID v2 tokens, which allows remote authenticated users to bypass the token expiration and retain access via a verification (1) GET or (2) HEAD request to v3/auth/tokens/.	openstack keystone	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2066
7149	CVE-2014-5251	Medium		The MySQL token driver in OpenStack Identity (Keystone) 2014.1.x before 2014.1.2.1 and Juno before Juno-3 stores timestamps with the incorrect precision, which causes the expiration comparison for tokens to fail and allows remote authenticated users to retain access via an expired token.	openstack keystone	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2073
7150	CVE-2014-5220			The mdcheck script of the mdadm package for openSUSE 13.2 prior to version 3.3.1-5.14.1 does not properly sanitize device names, which allows local attackers to execute arbitrary commands as root.	mdadm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4104
7151	CVE-2014-5207	Medium		fs/namespace.c in the Linux kernel through 3.16.1 does not properly restrict clearing MNT_NODEV, MNT_NOSUID, and MNT_NOEXEC and changing MNT_ATIME_MASK during a remount of a bind mount, which allows local users to gain privileges, interfere with backups and auditing on systems that had atime enabled, or cause a denial of service (excessive filesystem updating) on systems that had atime disabled via a mount -o remount command within a user namespace.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8283
7152	CVE-2014-5206	High		The do_remount function in fs/namespace.c in the Linux kernel through 3.16.1 does not maintain the MNT_LOCK_READONLY bit across a remount of a bind mount, which allows local users to bypass an intended read-only restriction and defeat certain sandbox protection mechanisms via a mount -o remount command within a user namespace.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8273
7153	CVE-2014-5177	Low		libvirt 1.0.0 through 1.2.x before 1.2.5, when fine grained access control is enabled, allows local users to read arbitrary files via a crafted XML document containing an XML external entity declaration in conjunction with an entity reference to the (1) virDomainDefineXML, (2) virNetworkCreateXML, (3) virNetworkDefineXML, (4) virStoragePoolCreateXML, (5) virStoragePoolDefineXML, (6) virStorageVolCreateXML, (7) virDomainCreateXML, (8) virNodeDeviceCreateXML, (9) virInterfaceDefineXML, (10) virStorageVolCreateXMLFrom, (11) virConnectDomainXMLFromNative, (12) virConnectDomainXMLToNative, (13) virSecretDefineXML, (14) virNWFilterDefineXML, (15) virDomainSnapshotCreateXML, (16) virDomainSaveImageDefineXML, (17) virDomainCreateXMLWithFiles, (18) virConnectCompareCPU, or (19) virConnectBaselineCPU API method, related to an XML External Entity (XXE) issue. NOTE: this issue was SPLIT from CVE-2014-0179 per ADT3 due to different affected versions of some vectors.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8185
7154	CVE-2014-5149	Medium		Certain MMU virtualization operations in Xen 4.2.x through 4.4.x, when using shadow pagetables, are not preemptible, which allows local HVM guest to cause a denial of service (vcpu consumption) by invoking these operations, which process every page assigned to a guest, a different vulnerability than CVE-2014-5146.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2070

	A	B	C	D	E	F	G	H	I	J	K	L	M
7155	CVE-2014-5147	MEDIUM		Xen 4.4.x, when running a 64-bit kernel on an ARM system, does not properly handle traps from the guest domain that use a different address width, which allows local guest users to cause a denial of service (host crash) via a crafted 32-bit process.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2067
7156	CVE-2014-5146	Medium		Certain MMU virtualization operations in Xen 4.2.x through 4.4.x before the xsa97-hap patch, when using Hardware Assisted Paging (HAP), are not preemptible, which allows local HVM guest to cause a denial of service (vcpu consumption) by invoking these operations, which process every page assigned to a guest, a different vulnerability than CVE-2014-5149.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2071
7157	CVE-2014-5139	MEDIUM		The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL servers to cause a denial of service (NULL pointer dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite without the required negotiation of that ciphersuite with the client.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8146
7158	CVE-2014-5120	Medium		gd_ctx.c in the GD component in PHP 5.4.x before 5.4.32 and 5.5.x before 5.5.16 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to overwrite arbitrary files via crafted input to an application that calls the (1) imagegd, (2) imagegd2, (3) imagegif, (4) imagejpeg, (5) imagepng, (6) imagewbmp, or (7) imagewebp function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8279
7159	CVE-2014-5119	HIGH		Off-by-one error in the __gconv_translit_find function in gconv_trans.c in GNU C Library (aka glibc) allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via vectors related to the CHARSET environment variable and gconv transliteration modules.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8271
7160	CVE-2014-5077	Medium		The sctp_assoc_update function in net/sctp/associola.c in the Linux kernel through 3.15.8, when SCTP authentication is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and OOPS) by starting to establish an association between two endpoints immediately after an exchange of INIT and INIT ACK chunks to establish an earlier association between these endpoints in the opposite direction.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8083
7161	CVE-2014-5045	Medium		The mountpoint_last function in fs/namei.c in the Linux kernel before 3.15.8 does not properly maintain a certain reference count during attempts to use the umount system call in conjunction with a symlink, which allows local users to cause a denial of service (memory consumption or use-after-free) or possibly have unspecified other impact via the umount program.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8064
7162	CVE-2014-4987	Medium		server_user_groups.php in phpMyAdmin 4.1.x before 4.1.14.2 and 4.2.x before 4.2.6 allows remote authenticated users to bypass intended access restrictions and read the MySQL user list via a viewUsers request.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8062
7163	CVE-2014-4986	Low		Multiple cross-site scripting (XSS) vulnerabilities in js/functions.js in phpMyAdmin 4.0.x before 4.0.10.1, 4.1.x before 4.1.14.2, and 4.2.x before 4.2.6 allow remote authenticated users to inject arbitrary web script or HTML via a crafted (1) table name or (2) column name that is improperly handled during construction of an AJAX confirmation message.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8068
7164	CVE-2014-4955	Low		Cross-site scripting (XSS) vulnerability in the PMA_TRI_getRowForList function in libraries/rte/rte_list.lib.php in phpMyAdmin 4.0.x before 4.0.10.1, 4.1.x before 4.1.14.2, and 4.2.x before 4.2.6 allows remote authenticated users to inject arbitrary web script or HTML via a crafted trigger name that is improperly handled on the database triggers page.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8074
7165	CVE-2014-4954	Low		Cross-site scripting (XSS) vulnerability in the PMA_getHtmlForActionLinks function in libraries/structure.lib.php in phpMyAdmin 4.2.x before 4.2.6 allows remote authenticated users to inject arbitrary web script or HTML via a crafted table comment that is improperly handled during construction of a database structure page.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8080
7166	CVE-2014-4943	Medium		The PPPoL2TP feature in net/l2tp/l2tp_ppp.c in the Linux kernel through 3.15.6 allows local users to gain privileges by leveraging data-structure differences between an l2tp socket and an inet socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8072
7167	CVE-2014-4910	Medium		Directory traversal vulnerability in tools/backlight_helper.c in X.Org xf86-video-intel 2.99.911 allows remote attackers to create or overwrite arbitrary files via a .. (dot dot) in the interface name.	xf86-video-intel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8088
7168	CVE-2014-4877	High		Absolute path traversal vulnerability in GNU Wget before 1.16, when recursion is enabled, allows remote FTP servers to write to arbitrary files, and consequently execute arbitrary code, via a LIST response that references the same filename within two entries, one of which indicates that the filename is for a symlink.	wget	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2140
7169	CVE-2014-4721	Low		The phpinfo implementation in ext/standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not ensure use of the string data type for the PHP_AUTH_PW, PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might allow context-dependent attackers to obtain sensitive information from process memory by using the integer data type with crafted values, related to a type confusion vulnerability, as demonstrated by reading a private SSL key in an Apache HTTP Server web-hosting environment with mod_ssl and a PHP 5.3.x mod_php.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7958

	A	B	C	D	E	F	G	H	I	J	K	L	M
7170	CVE-2014-4699	Medium		The Linux kernel before 3.15.4 on Intel processors does not properly restrict use of a non-canonical value for the saved RIP address in the case of a system call that does not use IRET, which allows local users to leverage a race condition and gain privileges, or cause a denial of service (double fault), via a crafted application that makes ptrace and fork system calls.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7962
7171	CVE-2014-4698	Medium		Use-after-free vulnerability in ext/spl/spl_array.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted ArrayIterator usage within applications in certain web-hosting environments.CWE-416: Use After Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7951
7172	CVE-2014-4670	Medium		Use-after-free vulnerability in ext/spl/spl_dllist.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted iterator usage within applications in certain web-hosting environments.CWE-416: Use After Free	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7949
7173	CVE-2014-4667	Medium		The sctp_association_free function in net/sctp/associola.c in the Linux kernel before 3.15.2 does not properly manage a certain backlog value, which allows remote attackers to cause a denial of service (socket outage) via a crafted SCTP packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7960
7174	CVE-2014-4656	Medium		Multiple integer overflows in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 allow local users to cause a denial of service by leveraging /dev/snd/controlCX access, related to (1) index values in the snd_ctl_add function and (2) numid values in the snd_ctl_remove_numid_conflict function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7947
7175	CVE-2014-4655	Medium		The snd_ctl_elem_add function in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 does not properly maintain the user_ctl_count value, which allows local users to cause a denial of service (integer overflow and limit bypass) by leveraging /dev/snd/controlCX access for a large number of SNDRV_CTL_IOCTL_ELEM_REPLACE ioctl calls.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7963
7176	CVE-2014-4654	Medium		The snd_ctl_elem_add function in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 does not check authorization for SNDRV_CTL_IOCTL_ELEM_REPLACE commands, which allows local users to remove kernel controls and cause a denial of service (use-after-free and system crash) by leveraging /dev/snd/controlCX access for an ioctl call.CWE-416: Use After Free	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7953
7177	CVE-2014-4653	Medium		sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 does not ensure possession of a read/write lock, which allows local users to cause a denial of service (use-after-free) and obtain sensitive information from kernel memory by leveraging /dev/snd/controlCX access.CWE-416: Use After Free	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7948
7178	CVE-2014-4652	Medium		Race condition in the tlv handler functionality in the snd_ctl_elem_user_tlv function in sound/core/control.c in the ALSA control implementation in the Linux kernel before 3.15.2 allows local users to obtain sensitive information from kernel memory by leveraging /dev/snd/controlCX access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7957
7179	CVE-2014-4617	Medium		The do_uncompress function in g10/compress.c in GnuPG 1.x before 1.4.17 and 2.x before 2.0.24 allows context-dependent attackers to cause a denial of service (infinite loop) via malformed compressed packets, as demonstrated by an a3 01 5b ff byte sequence.	gnupg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7797
7180	CVE-2014-4616			It was reported [1] that Python built-in _json module have a flaw (insufficient bounds checking), which allows a local user to read current process' arbitrary memory.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-972
7181	CVE-2014-4615	Medium		The notifier middleware in OpenStack PyCADF 0.5.0 and earlier, Telemetry (Ceilometer) 2013.2 before 2013.2.4 and 2014.x before 2014.1.2, Neutron 2014.x before 2014.1.2 and Juno before Juno-2, and Oslo allows remote authenticated users to obtain X_AUTH_TOKEN values by reading the message queue (v2/meters/http.request).	openstack pycadf	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2065
7182	CVE-2014-4611	Medium		Integer overflow in the LZ4 algorithm implementation, as used in Yann Collet LZ4 before r118 and in the lz4_uncompress function in lib/lz4/lz4_decompress.c in the Linux kernel before 3.15.2, on 32-bit platforms might allow context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted Literal Run that would be improperly handled by programs not complying with an API limitation, a different vulnerability than CVE-2014-4715.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7961
7183	CVE-2014-4608	Medium		** DISPUTED ** Multiple integer overflows in the lzo1x_decompress_safe function in lib/lzo/lzo1x_decompress_safe.c in the LZO decompressor in the Linux kernel before 3.15.2 allow context-dependent attackers to cause a denial of service (memory corruption) via a crafted Literal Run. NOTE: the author of the LZO algorithms says the Linux kernel is *not* affected; media hype.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7952

	A	B	C	D	E	F	G	H	I	J	K	L	M
7184	CVE-2014-4607			An integer overflow may occur when processing any variant of a "literal run" in the lzo1x_decompress_safe function. Each of these three locations is subject to an integer overflow when processing zero bytes. This exposes the code that copies literals to memory corruption. It should be noted that if the target is 64bit liblzo2, the overflow is still possible, but impractical. An overflow would require so much input data that an attack would be infeasible even in modern computers. This issue is LAZARUS.1	busybox	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-367
7185	CVE-2014-4508	Medium		arch/x86/kernel/entry_32.S in the Linux kernel through 3.15.1 on 32-bit x86 platforms, when syscall auditing is enabled and the sep CPU feature flag is set, allows local users to cause a denial of service (OOPS and system crash) via an invalid syscall number, as demonstrated by number 1000.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7799
7186	CVE-2014-4349	Low		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.1.x before 4.1.14.1 and 4.2.x before 4.2.4 allow remote authenticated users to inject arbitrary web script or HTML via a crafted table name that is improperly handled after a (1) hide or (2) unhide action.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7790
7187	CVE-2014-4348	Low		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 4.2.x before 4.2.4 allow remote authenticated users to inject arbitrary web script or HTML via a crafted (1) database name or (2) table name that is improperly handled after presence in (a) the favorite list or (b) recent tables.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7788
7188	CVE-2014-4345	HIGH		Off-by-one error in the krb5_encode_krbsecretkey function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in kadmind in MIT Kerberos 5 (aka krb5) 1.6.x through 1.11.x before 1.11.6 and 1.12.x before 1.12.2 allows remote authenticated users to cause a denial of service (buffer overflow) or possibly execute arbitrary code via a series of cpw -keepold commands.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8182
7189	CVE-2014-4344	HIGH		The acc_ctx_cont function in the SPNEGO acceptor in lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) 1.5.x through 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty continuation token at a certain point during a SPNEGO negotiation.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8187
7190	CVE-2014-4343	HIGH		Double free vulnerability in the init_ctx_reselect function in the SPNEGO initiator in lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) 1.10.x through 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via network traffic that appears to come from an intended acceptor, but specifies a security mechanism different from the one proposed by the initiator.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8184
7191	CVE-2014-4342	Medium		MIT Kerberos 5 (aka krb5) 1.7.x through 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (buffer over-read or NULL pointer dereference, and application crash) by injecting invalid tokens into a GSSAPI application session.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8084
7192	CVE-2014-4341	Medium		MIT Kerberos 5 (aka krb5) before 1.12.2 allows remote attackers to cause a denial of service (buffer over-read and application crash) by injecting invalid tokens into a GSSAPI application session.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8092
7193	CVE-2014-4330	Low		The Dumper method in Data::Dumper before 2.154, as used in Perl 5.20.1 and earlier, allows context-dependent attackers to cause a denial of service (stack consumption and crash) via an Array-Reference with many nested Array-References, which triggers a large number of recursive calls to the DD_dump function.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8551
7194	CVE-2014-4323	High		The mdp_lut_hw_update function in drivers/video/msm/mdp.c in the MDP display driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not validate certain start and length values within an ioctl call, which allows attackers to gain privileges via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2429
7195	CVE-2014-4322	High		drivers/misc/qseecom.c in the QSEECOM driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not validate certain offset, length, and base values within an ioctl call, which allows attackers to gain privileges or cause a denial of service (memory corruption) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2570
7196	CVE-2014-4287	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier and 5.6.19 and earlier allows remote authenticated users to affect availability via vectors related to SERVER:CHARACTER SETS.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8666
7197	CVE-2014-4274	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.38 and earlier and 5.6.19 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to SERVER:MyISAM.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8648
7198	CVE-2014-4260	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.37 and earlier, and 5.6.17 and earlier, allows remote authenticated users to affect integrity and availability via vectors related to SRCHAR.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8073
7199	CVE-2014-4258	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.37 and earlier and 5.6.17 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to SRINFOSC.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8085
7200	CVE-2014-4243	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.35 and earlier and 5.6.15 and earlier allows remote authenticated users to affect availability via vectors related to ENFED.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8090

	A	B	C	D	E	F	G	H	I	J	K	L	M
7201	CVE-2014-4240	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows local users to affect confidentiality and integrity via vectors related to SRREP.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8094
7202	CVE-2014-4238	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect availability via vectors related to SROPTZR.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8086
7203	CVE-2014-4233	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect availability via vectors related to SRREP.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8091
7204	CVE-2014-4214	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect availability via vectors related to SRSP.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8079
7205	CVE-2014-4207	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.37 and earlier allows remote authenticated users to affect availability via vectors related to SROPTZR.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8070
7206	CVE-2014-4171	Medium		mm/shmem.c in the Linux kernel through 3.15.1 does not properly implement the interaction between range notification and hole punching, which allows local users to cause a denial of service (i_mutex hold) by using the mmap system call to access a hole, as demonstrated by interfering with intended shmem activity by blocking completion of (1) an MADV_REMOVE madvise call or (2) an FALLOC_FL_PUNCH_HOLE fallocate call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7801
7207	CVE-2014-4167	Low		The L3-agent in OpenStack Neutron before 2013.2.4, 2014.x before 2014.1.2, and Juno before Juno-2 allows remote authenticated users to cause a denial of service (IPv4 address attachment outage) by attaching an IPv6 private subnet to a L3 router.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1985
7208	CVE-2014-4165	Medium		Cross-site scripting (XSS) vulnerability in ntop allows remote attackers to inject arbitrary web script or HTML via the title parameter in a list action to plugins/rrdPlugin.	ntop	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	CGP6-477
7209	CVE-2014-4157	Medium		arch/mips/include/asm/thread_info.h in the Linux kernel before 3.14.8 on the MIPS platform does not configure _TIF_SECCOMP checks on the fast system-call path, which allows local users to bypass intended PR_SET_SECCOMP restrictions by executing a crafted application without invoking a trace or audit subsystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7786
7210	CVE-2014-4049	Medium		Heap-based buffer overflow in the php_parserr function in ext/standard/dns.c in PHP 5.6.0beta4 and earlier allows remote servers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted DNS TXT record, related to the dns_get_record function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7794
7211	CVE-2014-4043	High		The posix_spawn_file_actions_addopen function in glibc before 2.20 does not copy its path argument in accordance with the POSIX specification, which allows context-dependent attackers to trigger use-after-free vulnerabilities.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5193
7212	CVE-2014-4027	Low		The rd_build_device_space function in drivers/target/target_core_rd.c in the Linux kernel before 3.14 does not properly initialize a certain data structure, which allows local users to obtain sensitive information from ramdisk_mcp memory by leveraging access to a SCSI initiator.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7800
7213	CVE-2014-4022	Low		The alloc_domain_struct function in arch/arm/domain.c in Xen 4.4.x, when running on an ARM platform, does not properly initialize the structure containing the grant table pages for a domain, which allows local guest administrators to obtain sensitive information via the GNTTABOP_setup_table subhypercall.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1988
7214	CVE-2014-4021	Low		Xen 3.2.x through 4.4.x does not properly clean memory pages recovered from guests, which allows local guest OS users to obtain sensitive information via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1959
7215	CVE-2014-4014	High		The capabilities implementation in the Linux kernel before 3.14.8 does not properly consider that namespaces are inapplicable to inodes, which allows local users to bypass intended chmod restrictions by first creating a user namespace, as demonstrated by setting the setgid bit on a file with group ownership of root.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7796
7216	CVE-2014-3981	Low		acinclude.m4, as used in the configure script in PHP 5.5.13 and earlier, allows local users to overwrite arbitrary files via a symlink attack on the /tmp/phpglibccheck file.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7669
7217	CVE-2014-3970	Low		The pa_rtp_recv function in modules/rtp/rtp.c in the module-rtp-recv module in PulseAudio 5.0 and earlier allows remote attackers to cause a denial of service (assertion failure and abort) via an empty UDP packet.	pulseaudio	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7672
7218	CVE-2014-3969	High		Xen 4.4.x, when running on an ARM system, does not properly check write permissions on virtual addresses, which allows local guest administrators to gain privileges via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1934
7219	CVE-2014-3968	Medium		The HVMOP_inject_msi function in Xen 4.2.x, 4.3.x, and 4.4.x allows local guest HVM administrators to cause a denial of service (host crash) via a large number of crafted requests, which trigger an error messages to be logged.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1930
7220	CVE-2014-3967	Medium		The HVMOP_inject_msi function in Xen 4.2.x, 4.3.x, and 4.4.x does not properly check the return value from the IRQ setup check, which allows local HVM guest administrators to cause a denial of service (NULL pointer dereference and crash) via unspecified vectors.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1926

	A	B	C	D	E	F	G	H	I	J	K	L	M
7221	CVE-2014-3940	Medium		The Linux kernel through 3.14.5 does not properly consider the presence of hugetlb entries, which allows local users to cause a denial of service (memory corruption or system crash) by accessing certain memory locations, as demonstrated by triggering a race condition via numa_maps read operations during hugepage migration, related to fs/proc/task_mmu.c and mm/mempolicy.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7677
7222	CVE-2014-3925	Medium		sosreport in Red Hat sos 1.7 and earlier on Red Hat Enterprise Linux (RHEL) 5 produces an archive with an fstab file potentially containing cleartext passwords, and lacks a warning about reviewing this archive to detect included passwords, which might allow remote attackers to obtain sensitive information by leveraging access to a technical-support data stream.	sosreport	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2005
7223	CVE-2014-3917	Low		kernel/auditsc.c in the Linux kernel through 3.14.5, when CONFIG_AUDITSYSCALL is enabled with certain syscall rules, allows local users to obtain potentially sensitive single-bit values from kernel memory or cause a denial of service (OOPS) via a large value of a syscall number.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7678
7224	CVE-2014-3859	Medium		libdns in ISC BIND 9.10.0 before P2 does not properly handle EDNS options, which allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a crafted packet, as demonstrated by an attack against named, dig, or delv.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7787
7225	CVE-2014-3801	Low		OpenStack Orchestration API (Heat) 2013.2 through 2013.2.3 and 2014.1, when creating the stack for a template using a provider template, allows remote authenticated users to obtain the provider template URL via the resource-type-list.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1915
7226	CVE-2014-3717	Low		Xen 4.4.x does not properly validate the load address for 64-bit ARM guest kernels, which allows local users to read system memory or cause a denial of service (crash) via a crafted kernel, which triggers a buffer overflow.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1909
7227	CVE-2014-3716	Low		Xen 4.4.x does not properly check alignment, which allows local users to cause a denial of service (crash) via an unspecified field in a DTB header in a 32-bit guest kernel.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1910
7228	CVE-2014-3715	Low		Buffer overflow in Xen 4.4.x allows local users to read system memory or cause a denial of service (crash) via a crafted 32-bit guest kernel, related to searching for an appended DTB.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1912
7229	CVE-2014-3714	Low		The ARM image loading functionality in Xen 4.4.x does not properly validate kernel length, which allows local users to read system memory or cause a denial of service (crash) via a crafted 32-bit ARM guest kernel in an image, which triggers a buffer overflow.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1914
7230	CVE-2014-3710	Medium		The donote function in readelf.c in file through 5.20, as used in the Fileinfo component in PHP 5.4.34, does not ensure that sufficient note headers are present, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted ELF file.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2116
7231	CVE-2014-3707	MEDIUM		The curl_easy_duphandle function in libcurl 7.17.1 through 7.38.0, when running with the CURLOPT_COPYPOSTFIELDS option, does not properly copy HTTP POST data for an easy handle, which triggers an out-of-bounds read that allows remote web servers to read sensitive memory information.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8748
7232	CVE-2014-3703	Medium		OpenStack PackStack 2012.2.1, when the Open vSwitch (OVS) monolithic plug-in is not used, does not properly set the libvirt_vif_driver configuration option when generating the nova.conf configuration, which causes the firewall to be disabled and allows remote attackers to bypass intended access restrictions.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2263
7233	CVE-2014-3690	Medium		arch/x86/kvm/vmx.c in the KVM subsystem in the Linux kernel before 3.17.2 on Intel processors does not ensure that the value in the CR4 control register remains the same after a VM entry, which allows host OS users to kill arbitrary processes or cause a denial of service (system disruption) by leveraging /dev/kvm access, as demonstrated by PR_SET_TSC prctl calls within a modified copy of QEMU.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8738
7234	CVE-2014-3689	High		The vmware-vga driver (hw/display/vmware_vga.c) in QEMU allows local guest users to write to qemu memory locations and gain privileges via unspecified parameters related to rectangle handling.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2153
7235	CVE-2014-3688	MEDIUM		The SCTP implementation in the Linux kernel before 3.17.4 allows remote attackers to cause a denial of service (memory consumption) by triggering a large number of chunks in an association's output queue, as demonstrated by ASCONF probes, related to net/sctp/inqueue.c and net/sctp/sm_statefuns.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2126
7236	CVE-2014-3687	High		The sctp_assoc_lookup_asconf_ack function in net/sctp/associola.c in the SCTP implementation in the Linux kernel through 3.17.2 allows remote attackers to cause a denial of service (panic) via duplicate ASCONF chunks that trigger an incorrect uncork within the side-effect interpreter.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2149
7237	CVE-2014-3686	Medium		wpa_supplicant and hostapd 0.7.2 through 2.2, when running with certain configurations and using wpa_cli or hostapd_cli with action scripts, allows remote attackers to execute arbitrary commands via a crafted frame.	hostapd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8654
7238	CVE-2014-3683	Medium		Integer overflow in rsyslog before 7.6.7 and 8.x before 8.4.2 and sysklogd 1.5 and earlier allows remote attackers to cause a denial of service (crash) via a large priority (PRI) value. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-3634.	sysklogd & rsyslog	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2098
7239	CVE-2014-3673	High		The SCTP implementation in the Linux kernel through 3.17.2 allows remote attackers to cause a denial of service (system crash) via a malformed ASCONF chunk, related to net/sctp/sm_make_chunk.c and net/sctp/sm_statefuns.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2108

	A	B	C	D	E	F	G	H	I	J	K	L	M
7240	CVE-2014-3672	Low		The qemu implementation in libvirt before 1.3.0 and Xen allows local guest OS users to cause a denial of service (host disk consumption) by writing to stdout or stderr.	libvirt	Unchanged	Not vulnerable	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-731
7241	CVE-2014-3670	Medium		The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2135
7242	CVE-2014-3669	High		Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2129
7243	CVE-2014-3668	Medium		Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) via (1) a crafted first argument to the xmlrpc_set_type function or (2) a crafted argument to the xmlrpc_decode function, related to an out-of-bounds read operation.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2157
7244	CVE-2014-3660	Medium		parser.c in libxml2 before 2.9.2 does not properly prevent entity expansion even when entity substitution has been disabled, which allows context-dependent attackers to cause a denial of service (CPU consumption) via a crafted XML document containing a large number of nested entity references, a variant of the billion laughs attack.CWE-611: Improper Restriction of XML External Entity Reference ('XXE')	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8743
7245	CVE-2014-3657	Medium		The virDomainListPopulate function in conf/domain_conf.c in libvirt before 1.2.9 does not clean up the lock on the list of domains, which allows remote attackers to cause a denial of service (deadlock) via a NULL value in the second parameter in the virConnectListAllDomains API command.	libvirt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8556
7246	CVE-2014-3647	Low		arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel through 3.17.2 does not properly perform RIP changes, which allows guest OS users to cause a denial of service (guest OS crash) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2162
7247	CVE-2014-3646	Low		arch/x86/kvm/vmx.c in the KVM subsystem in the Linux kernel through 3.17.2 does not have an exit handler for the INVVPID instruction, which allows guest OS users to cause a denial of service (guest OS crash) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2134
7248	CVE-2014-3645	Low		arch/x86/kvm/vmx.c in the KVM subsystem in the Linux kernel before 3.12 does not have an exit handler for the INVEPT instruction, which allows guest OS users to cause a denial of service (guest OS crash) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2102
7249	CVE-2014-3641	Medium		The (1) GlusterFS and (2) Linux Smbfs drivers in OpenStack Cinder before 2014.1.3 allows remote authenticated users to obtain file data from the Cinder-volume host by cloning and attaching a volume with a crafted qcow2 header.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2162
7250	CVE-2014-3640	Low		The sosendto function in slirp/udp.c in QEMU before 2.1.2 allows local users to cause a denial of service (NULL pointer dereference) by sending a udp packet with a value of 0 in the source port and address, which triggers access of an uninitialized socket.CWE-476: NULL Pointer Dereference	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8756
7251	CVE-2014-3638	Low		The bus_connections_check_reply function in config-parser.c in D-Bus before 1.6.24 and 1.8.x before 1.8.8 allows local users to cause a denial of service (CPU consumption) via a large number of method calls.	dbus	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8554
7252	CVE-2014-3637	Low		D-Bus 1.3.0 through 1.6.x before 1.6.24 and 1.8.x before 1.8.8 does not properly close connections for processes that have terminated, which allows local users to cause a denial of service via a D-bus message containing a D-Bus connection file descriptor.CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime	dbus	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8538
7253	CVE-2014-3636	Low		D-Bus 1.3.0 through 1.6.x before 1.6.24 and 1.8.x before 1.8.8 allows local users to (1) cause a denial of service (prevention of new connections and connection drop) by queuing the maximum number of file descriptors or (2) cause a denial of service (disconnect) via multiple messages that combine to have more than the allowed number of file descriptors for a single sendmsg call.	dbus	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8676
7254	CVE-2014-3635	Medium		Off-by-one error in D-Bus 1.3.0 through 1.6.x before 1.6.24 and 1.8.x before 1.8.8, when running on a 64-bit system and the max_message_unix_fds limit is set to an odd number, allows remote attackers to cause a denial of service (dbus-daemon crash) or possibly execute arbitrary code by sending one more file descriptor than the limit, which triggers a heap-based buffer overflow or an assertion failure.	dbus	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8545
7255	CVE-2014-3634	High		rsyslog before 7.6.6 and 8.x before 8.4.1 and sysklogd 1.5 and earlier allows remote attackers to cause a denial of service (crash), possibly execute arbitrary code, or have other unspecified impact via a crafted priority (PRI) value that triggers an out-of-bounds array access.	sysklogd & rsyslog	Unchanged	8.0.0.2	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2109

	A	B	C	D	E	F	G	H	I	J	K	L	M
7256	CVE-2014-3633	Medium		The qemuDomainGetBlockIoTune function in qemu/qemu_driver.c in libvirt before 1.2.9, when a disk has been hot-plugged or removed from the live image, allows remote attackers to cause a denial of service (crash) or read sensitive heap information via a crafted blkiotune query, which triggers an out-of-bounds read.	libvirt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8539
7257	CVE-2014-3632	High		The default configuration in a sudoers file in the Red Hat openstack-neutron package before 2014.1.2-4, as used in Red Hat Enterprise Linux Open Stack Platform 5.0 for Red Hat Enterprise Linux 6, allows remote attackers to gain privileges via a crafted configuration file. NOTE: this vulnerability exists because of a CVE-2013-6433 regression.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2173
7258	CVE-2014-3631	High		The assoc_array_gc function in the associative-array implementation in lib/assoc_array.c in the Linux kernel before 3.16.3 does not properly implement garbage collection, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via multiple keyctl newring operations followed by a keyctl timeout operation.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8562
7259	CVE-2014-3621	Medium		The catalog url replacement in Keystone before 2013.2.3 and 2014.1 before 2014.1.2.1 allows remote authenticated users to read sensitive configuration options via a crafted endpoint, as demonstrated by $(admin_token) in the publicurl endpoint field.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2167
7260	CVE-2014-3620	MEDIUM		http://curl.haxx.se/docs/adv_20140910B.html	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8645
7261	CVE-2014-3616	Medium		nginx 0.5.6 through 1.7.4, when using the same shared ssl_session_cache or ssl_session_ticket_key for multiple servers, can reuse a cached SSL session for an unrelated context, which allows remote attackers with certain privileges to conduct virtual host confusion attacks.	nginx	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2446
7262	CVE-2014-3615	Low		The VGA emulator in QEMU allows local guest users to read host memory by setting the display to a high resolution.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2100
7263	CVE-2014-3613	MEDIUM		http://curl.haxx.se/docs/adv_20140910A.html	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8603
7264	CVE-2014-3611	Medium		Race condition in the __kvm_migrate_pit_timer function in arch/x86/kvm/i8254.c in the KVM subsystem in the Linux kernel through 3.17.2 allows guest OS users to cause a denial of service (host OS crash) by leveraging incorrect PIT emulation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2139
7265	CVE-2014-3610	Medium		The WRMSR processing functionality in the KVM subsystem in the Linux kernel through 3.17.2 does not properly handle the writing of a non-canonical address to a model-specific register, which allows guest OS users to cause a denial of service (host OS crash) by leveraging guest OS privileges, related to the wrmsr_interception function in arch/x86/kvm/svm.c and the handle_wrmsr function in arch/x86/kvm/vmx.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2106
7266	CVE-2014-3608	Low		The VMWare driver in OpenStack Compute (Nova) before 2014.1.3 allows remote authenticated users to bypass the quota limit and cause a denial of service (resource consumption) by putting the VM into the rescue state, suspending it, which puts into an ERROR state, and then deleting the image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-2573.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2163
7267	CVE-2014-3601	Medium		The kvm_iommu_map_pages function in virt/kvm/iommu.c in the Linux kernel through 3.16.1 miscalculates the number of pages during the handling of a mapping failure, which allows guest OS users to (1) cause a denial of service (host OS memory corruption) or possibly have unspecified other impact by triggering a large gfn value or (2) cause a denial of service (host OS memory consumption) by triggering a small gfn value that leads to permanently pinned pages.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8416
7268	CVE-2014-3597	Medium		Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8272
7269	CVE-2014-3591			Libgcrypt version 1.6.3 [1] and GnuPG version 1.4.19 [2] fix a side-channel attack which can potentially lead to an information leak. This issue is different from CVE-2014-5270.	libgcrypt & gnupg2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-366
7270	CVE-2014-3587	Medium		Integer overflow in the cdf_read_property_info function in cdf.c in file through 5.19, as used in the Fileinfo component in PHP before 5.4.32 and 5.5.x before 5.5.16, allows remote attackers to cause a denial of service (application crash) via a crafted CDF file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1571.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8278
7271	CVE-2014-3583	Medium		The handle_headers function in mod_proxy_fcgi.c in the mod_proxy_fcgi module in the Apache HTTP Server 2.4.10 allows remote FastCGI servers to cause a denial of service (buffer over-read and daemon crash) via long response headers.	apache	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2568
7272	CVE-2014-3581	MEDIUM		The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8549

	A	B	C	D	E	F	G	H	I	J	K	L	M
7273	CVE-2014-3580	Medium		The mod_dav_svn Apache HTTPD server module in Apache Subversion 1.x before 1.7.19 and 1.8.x before 1.8.11 allows remote attackers to cause a denial of service (NULL pointer dereference and server crash) via a REPORT request for a resource that does not exist.CWE-476: NULL Pointer Dereference	subversion	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2576
7274	CVE-2014-3572	Medium		The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-91
7275	CVE-2014-3571	Medium		OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.CWE-476: NULL Pointer Dereference	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-81
7276	CVE-2014-3570	Medium		The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-92
7277	CVE-2014-3569	Medium		The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling. NOTE: this issue became relevant after the CVE-2014-3568 fix.CWE-476: NULL Pointer Dereference	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2575
7278	CVE-2014-3568	Medium		OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8581
7279	CVE-2014-3567	High		Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8601
7280	CVE-2014-3566	Medium		The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the POODLE issue.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8579
7281	CVE-2014-3565	Medium		snmplib/mib.c in net-snmp 5.7.0 and earlier, when the -OQ option is used, allows remote attackers to cause a denial of service (snmptrapd crash) via a crafted SNMP trap message, which triggers a conversion to the variable type designated in the MIB file, as demonstrated by a NULL type in an ifMtu trap message.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8547
7282	CVE-2014-3564	Medium		Multiple heap-based buffer overflows in the status_handler function in (1) engine-gpgsm.c and (2) engine-uiserver.c in GPGME before 1.5.1 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to different line lengths in a specific order.	gpgme	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8656
7283	CVE-2014-3560	High		NetBIOS name services daemon (nmbd) in Samba 4.0.x before 4.0.21 and 4.1.x before 4.1.11 allows remote attackers to execute arbitrary code via unspecified vectors that modify heap memory, involving a sizeof operation on an incorrect variable in the unstrcpy macro in string_wrappers.h.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8186
7284	CVE-2014-3556	MEDIUM		The STARTTLS implementation in mail/ngx_mail_smtp_handler.c in the SMTP proxy in nginx 1.5.x and 1.6.x before 1.6.1 and 1.7.x before 1.7.4 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a plaintext command injection attack, a similar issue to CVE-2011-0411.	nginx	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2574
7285	CVE-2014-3555	Medium		OpenStack Neutron before 2013.2.4, 2014.x before 2014.1.2, and Juno before Juno-2 allows remote authenticated users to cause a denial of service (crash or long firewall rule updates) by creating a large number of allowed address pairs.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2014
7286	CVE-2014-3539			base/oi/doa.py in the Rope library in CPython (aka Python) allows remote attackers to execute arbitrary code by leveraging an unsafe call to pickle.load.	python	Unchanged	Investigate	Investigate	Investigate	Investigate	Investigate	Not vulnerable	LIN10-3727
7287	CVE-2014-3537	Low		The web interface in CUPS before 1.7.4 allows local users in the lp group to read arbitrary files via a symlink attack on a file in /var/cache/cups/rss/.	cups	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8069
7288	CVE-2014-3535	High		include/linux/netdevice.h in the Linux kernel before 2.6.36 incorrectly uses macros for netdev_printk and its related logging implementation, which allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) by sending invalid packets to a VxLAN interface.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8548

	A	B	C	D	E	F	G	H	I	J	K	L	M
7289	CVE-2014-3534	High		arch/s390/kernel/ptrace.c in the Linux kernel before 3.15.8 on the s390 platform does not properly restrict address-space control operations in PTRACE_POKEUSR_AREA requests, which allows local users to obtain read and write access to kernel memory locations, and consequently gain privileges, via a crafted application that makes a ptrace system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8076
7290	CVE-2014-3532	Low		dbus 1.3.0 before 1.6.22 and 1.8.x before 1.8.6, when running on Linux 2.6.37-rc4 or later, allows local users to cause a denial of service (system-bus disconnect of other services or applications) by sending a message containing a file descriptor, then exceeding the maximum recursion depth before the initial message is forwarded.	dbus	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8066
7291	CVE-2014-3528	Medium		Apache Subversion 1.0.0 through 1.7.x before 1.7.17 and 1.8.x before 1.8.10 uses an MD5 hash of the URL and authentication realm to store cached credentials, which makes it easier for remote servers to obtain the credentials via a crafted authentication realm.	subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8282
7292	CVE-2014-3523	Medium		Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8078
7293	CVE-2014-3522	Medium		The Serf RA layer in Apache Subversion 1.4.0 through 1.7.x before 1.7.18 and 1.8.x before 1.8.10 does not properly handle wildcards in the Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof servers via a crafted certificate.CWE-297: Improper Validation of Certificate with Host Mismatch	subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8277
7294	CVE-2014-3517	Medium		api/metadata/handler.py in OpenStack Compute (Nova) before 2013.2.4, 2014.x before 2014.1.2, and Juno before Juno-2, when proxying metadata requests through Neutron, makes it easier for remote attackers to guess instance ID signatures via a brute-force attack that relies on timing differences in responses to instance metadata requests.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2049
7295	CVE-2014-3515	High		The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to type confusion issues in (1) ArrayObject and (2) SPLObjectStorage.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7946
7296	CVE-2014-3513	High		Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8582
7297	CVE-2014-3512	HIGH		Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A, or (3) B parameter.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8178
7298	CVE-2014-3511	MEDIUM		The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to force the use of TLS 1.0 by triggering ClientHello message fragmentation in communication between a client and server that both support later TLS versions, related to a protocol downgrade issue.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8172
7299	CVE-2014-3510	MEDIUM		The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8167
7300	CVE-2014-3509	MEDIUM		Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.1i, when multithreading and session resumption are used, allows remote SSL servers to cause a denial of service (memory overwrite and client application crash) or possibly have unspecified other impact by sending Elliptic Curve (EC) Supported Point Formats Extension data.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8156
7301	CVE-2014-3508	MEDIUM		The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8150
7302	CVE-2014-3507	MEDIUM		Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8163
7303	CVE-2014-3506	MEDIUM		d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8162

	A	B	C	D	E	F	G	H	I	J	K	L	M
7304	CVE-2014-3505	MEDIUM		Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8160
7305	CVE-2014-3504	Medium		The (1) serf_ssl_cert_issuer, (2) serf_ssl_cert_subject, and (3) serf_ssl_cert_certificate functions in Serf 0.2.0 through 1.3.x before 1.3.7 does not properly handle a NUL byte in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.CWE-297: Improper Validation of Certificate with Host Mismatch	serf	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-680
7306	CVE-2014-3497	Medium		Cross-site scripting (XSS) vulnerability in OpenStack Swift 1.11.0 through 1.13.1 allows remote attackers to inject arbitrary web script or HTML via the WWW-Authenticate header.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1983
7307	CVE-2014-3493	Low		The push_ascii function in smbd in Samba 3.6.x before 3.6.24, 4.0.x before 4.0.19, and 4.1.x before 4.1.9 allows remote authenticated users to cause a denial of service (memory corruption and daemon crash) via an attempt to read a Unicode pathname without specifying use of Unicode, leading to a character-set conversion failure that triggers an invalid pointer dereference.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7798
7308	CVE-2014-3487	Medium		The cdf_read_property_info function in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate a stream offset, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7956
7309	CVE-2014-3480	Medium		The cdf_count_chain function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate sector-count data, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7959
7310	CVE-2014-3479	Medium		The cdf_check_stream_offset function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, relies on incorrect sector-size data, which allows remote attackers to cause a denial of service (application crash) via a crafted stream offset in a CDF file.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7955
7311	CVE-2014-3478	Medium		Buffer overflow in the mconvert function in softmagic.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (application crash) via a crafted Pascal string in a FILE_PSTRING conversion.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7954
7312	CVE-2014-3477	Low		The dbus-daemon in D-Bus 1.2.x through 1.4.x, 1.6.x before 1.6.20, and 1.8.x before 1.8.4, sends an AccessDenied error to the service instead of a client when the client is prohibited from accessing the service, which allows local users to cause a denial of service (initialization failure and exit) or possibly conduct a side-channel attack via a D-Bus message to an inactive service.	dbus	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4963
7313	CVE-2014-3476	Medium		OpenStack Identity (Keystone) before 2013.2.4, 2014.1 before 2014.1.2, and Juno before Juno-2 does not properly handle chained delegation, which allows remote authenticated users to gain privileges by leveraging a (1) trust or (2) OAuth token with impersonation enabled to create a new token with additional roles.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1964
7314	CVE-2014-3471			Use-after-free vulnerability in hw/pci/pcie.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (QEMU instance crash) via hotplug and hotunplug operations of Virtio block devices.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3076
7315	CVE-2014-3470	Medium		The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7628
7316	CVE-2014-3469	Medium		The (1) asn1_read_value_type and (2) asn1_read_value functions in GNU Libtasn1 before 3.6 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) via a NULL value in an ivalue argument.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	libtasn1	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7648
7317	CVE-2014-3468	Medium		The asn1_get_bit_der function in GNU Libtasn1 before 3.6 does not properly report an error when a negative bit length is identified, which allows context-dependent attackers to cause out-of-bounds access via crafted ASN.1 data.	libtasn1	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7647
7318	CVE-2014-3467	Medium		Multiple unspecified vulnerabilities in the DER decoder in GNU Libtasn1 before 3.6, as used in GnutTLS, allow remote attackers to cause a denial of service (out-of-bounds read) via a crafted ASN.1 data.	libtasn1	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7646
7319	CVE-2014-3466	Medium		Buffer overflow in the read_server_hello function in lib/gnutls_handshake.c in GnuTLS before 3.1.25, 3.2.x before 3.2.15, and 3.3.x before 3.3.4 allows remote servers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a long session id in a ServerHello message.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7673

	A	B	C	D	E	F	G	H	I	J	K	L	M
7320	CVE-2014-3465	Medium		The gnutls_x509_dn_oid_name function in lib/x509/common.c in GnuTLS 3.0 before 3.1.20 and 3.2.x before 3.2.10 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted X.509 certificate, related to a missing LDAP description for an OID when printing the DN.Per http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7675
7321	CVE-2014-3461	Medium		hw/usb/bus.c in QEMU 1.6.2 allows remote attackers to execute arbitrary code via crafted savevm data, which triggers a heap-based buffer overflow, related to USB post load checks.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2159
7322	CVE-2014-3250			The default vhost configuration file in Puppet before 3.6.2 does not include the SSLCARevocationCheck directive, which might allow remote attackers to obtain sensitive information via a revoked certificate when a Puppet master runs with Apache 2.4.	puppet	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-2748
7323	CVE-2014-3227	Medium		dpkg 1.15.9, 1.16.x before 1.16.14, and 1.17.x before 1.17.9 expect the patch program to be compliant with a need for the C-style encoded filenames feature, but is supported in environments with noncompliant patch programs, which triggers an interaction error that allows remote attackers to conduct directory traversal attacks and modify files outside of the intended directories via a crafted source package. NOTE: this vulnerability exists because of reliance on unrealistic constraints on the behavior of an external program.	dpkg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7674
7324	CVE-2014-3215	Medium		seunshare in policycoreutils 2.2.5 is owned by root with 4755 permissions, and executes programs in a way that changes the relationship between the setuid system call and the getresuid saved set-user-ID value, which makes it easier for local users to gain privileges by leveraging a program that mistakenly expected that it could permanently drop privileges.	policycoreutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7432
7325	CVE-2014-3214	Medium		The prefetch implementation in named in ISC BIND 9.10.0, when a recursive nameserver is enabled, allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a DNS query that triggers a response with unspecified attributes.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7420
7326	CVE-2014-3185	Medium		Multiple buffer overflows in the command_port_read_callback function in drivers/usb/serial/whiteheat.c in the Whiteheat USB Serial Driver in the Linux kernel before 3.16.2 allow physically proximate attackers to execute arbitrary code or cause a denial of service (memory corruption and system crash) via a crafted device that provides a large amount of (1) EHCI or (2) XHCI data associated with a bulk response.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8561
7327	CVE-2014-3184	Medium		The report_fixup functions in the HID subsystem in the Linux kernel before 3.16.2 might allow physically proximate attackers to cause a denial of service (out-of-bounds write) via a crafted device that provides a small report descriptor, related to (1) drivers/hid/hid-cherry.c, (2) drivers/hid/hid-kye.c, (3) drivers/hid/hid-lg.c, (4) drivers/hid/hid-monterey.c, (5) drivers/hid/hid-petalynx.c, and (6) drivers/hid/hid-sunplus.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8553
7328	CVE-2014-3183	Medium		Heap-based buffer overflow in the logi_dj_ll_raw_request function in drivers/hid/hid-logitech-dj.c in the Linux kernel before 3.16.2 allows physically proximate attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a crafted device that specifies a large report size for an LED report.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8541
7329	CVE-2014-3182	Medium		Array index error in the logi_dj_raw_event function in drivers/hid/hid-logitech-dj.c in the Linux kernel before 3.16.2 allows physically proximate attackers to execute arbitrary code or cause a denial of service (invalid kfree) via a crafted device that provides a malformed REPORT_TYPE_NOTIF_DEVICE_UNPAIRED value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8537
7330	CVE-2014-3181	Medium		Multiple stack-based buffer overflows in the magicmouse_raw_event function in drivers/hid/hid-magicmouse.c in the Magic Mouse HID driver in the Linux kernel through 3.16.3 allow physically proximate attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a crafted device that provides a large amount of (1) EHCI or (2) XHCI data associated with an event.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8563
7331	CVE-2014-3158	High		Integer overflow in the getword function in options.c in pppd in Paul's PPP Package (ppp) before 2.4.7 allows attackers to access privileged options via a long word in an options file, which triggers a heap-based buffer overflow that [corrupts] security-relevant variables.	ppp	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2133
7332	CVE-2014-3153	High		The futex_requeue function in kernel/futex.c in the Linux kernel through 3.14.5 does not ensure that calls have two different futex addresses, which allows local users to gain privileges via a crafted FUTEX_REQUEUE command that facilitates unsafe waiter modification.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7666
7333	CVE-2014-3146	Medium		Incomplete blacklist vulnerability in the lxml.html.clean module in lxml before 3.3.5 allows remote attackers to conduct cross-site scripting (XSS) attacks via control characters in the link scheme to the clean_html function.Per: http://cwe.mitre.org/data/definitions/184.html CWE-184: Incomplete Blacklist	lxml	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	CGP6-473
7334	CVE-2014-3145	Medium		The BPF_S_ANC_NLATTR_NEST extension implementation in the sk_run_filter function in net/core/filter.c in the Linux kernel through 3.14.3 uses the reverse order in a certain subtraction, which allows local users to cause a denial of service (over-read and system crash) via crafted BPF instructions. NOTE: the affected code was moved to the __skb_get_nlattr_nest function before the vulnerability was announced.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7426

	A	B	C	D	E	F	G	H	I	J	K	L	M
7335	CVE-2014-3144	Medium		The (1) BPF_S_ANC_NLATTR and (2) BPF_S_ANC_NLATTR_NEST extension implementations in the sk_run_filter function in net/core/filter.c in the Linux kernel through 3.14.3 do not check whether a certain length value is sufficiently large, which allows local users to cause a denial of service (integer underflow and system crash) via crafted BPF instructions. NOTE: the affected code was moved to the __skb_get_nlattr and __skb_get_nlattr_nest functions before the vulnerability was announced.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7422
7336	CVE-2014-3127	High		dpkg 1.17.x before 1.17.9, 1.16.x before 1.16.14, and 1.15.x before 1.15.10 for Debian squeeze and wheezy supports C-style encoded filenames while the patch program does not, which introduces an interaction error that allows attackers to conduct directory traversal attacks and create files outside of the intended directories via a crafted package. NOTE: this vulnerability exists because of an incorrect fix for CVE-2014-0471.	dpkg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7417
7337	CVE-2014-3125	Medium		Xen 4.4.x, when running on an ARM system, does not properly context switch the CNTKCTL_EL1 register, which allows local guest users to modify the hardware timers and cause a denial of service (crash) via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1874
7338	CVE-2014-3124	Medium		The HVMOP_set_mem_type control in Xen 4.1 through 4.4.x allows local guest HVM administrators to cause a denial of service (hypervisor crash) or possibly execute arbitrary code by leveraging a separate qemu-dm vulnerability to trigger invalid page table translations for unspecified memory page types.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1870
7339	CVE-2014-3122	Medium		The try_to_unmap_cluster function in mm/rmap.c in the Linux kernel before 3.14.3 does not properly consider which pages must be locked, which allows local users to cause a denial of service (system crash) by triggering a memory-usage pattern that requires removal of page-table mappings.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7427
7340	CVE-2014-2986	Medium		The vgic_distr_mmio_write function in the virtual guest interrupt controller (GIC) distributor (arch/arm/vgic.c) in Xen 4.4.x, when running on an ARM system, allows local guest users to cause a denial of service (NULL pointer dereference and host crash) via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1865
7341	CVE-2014-2978	High		The Dispatch_Write function in proxy/dispatcher/idirectfbsurface_dispatcher.c in DirectFB 1.4.4 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the Voodoo interface, which triggers an out-of-bounds write.	directfb	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7668
7342	CVE-2014-2977	High		Multiple integer signedness errors in the Dispatch_Write function in proxy/dispatcher/idirectfbsurface_dispatcher.c in DirectFB 1.4.13 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the Voodoo interface, which triggers a stack-based buffer overflow.	directfb	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7670
7343	CVE-2014-2915	Medium		Xen 4.4.x, when running on ARM systems, does not properly restrict access to hardware features, which allows local guest users to cause a denial of service (host or guest crash) via unspecified vectors, related to (1) cache control, (2) coprocessors, (3) debug registers, and (4) other unspecified registers.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1830
7344	CVE-2014-2894	High		Off-by-one error in the cmd_smart function in the smart self test in hw/ide/core.c in QEMU before 2.0 allows local users to have unspecified impact via a SMART EXECUTE OFFLINE command that triggers a buffer underflow and memory corruption.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7292
7345	CVE-2014-2891	Medium		strongSwan before 5.1.2 allows remote attackers to cause a denial of service (NULL pointer dereference and IKE daemon crash) via a crafted ID_DER_ASN1_DN ID payload.	strongswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7424
7346	CVE-2014-2889	Medium		Off-by-one error in the bpf_jit_compile function in arch/x86/net/bpf_jit_comp.c in the Linux kernel before 3.1.8, when BPF JIT is enabled, allows local users to cause a denial of service (system crash) or possibly gain privileges via a long jump after a conditional jump.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7290
7347	CVE-2014-2856	Medium		Cross-site scripting (XSS) vulnerability in scheduler/client.c in Common Unix Printing System (CUPS) before 1.7.2 allows remote attackers to inject arbitrary web script or HTML via the URL path, related to the is_path_absolute function.	cups	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7280
7348	CVE-2014-2855	Medium		The check_secret function in authenticate.c in rsync 3.1.0 and earlier allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a user name which does not exist in the secrets file.	rsync	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7281
7349	CVE-2014-2851	Medium		Integer overflow in the ping_init_sock function in net/ipv4/ping.c in the Linux kernel through 3.14.1 allows local users to cause a denial of service (use-after-free and system crash) or possibly gain privileges via a crafted application that leverages an improperly managed reference counter.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7267
7350	CVE-2014-2830	High		Stack-based buffer overflow in cifskey.c or cifscreds.c in cifs-utils before 6.4, as used in pam_cifscreds, allows remote attackers to have unspecified impact via unknown vectors.	cifs-utils	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-291
7351	CVE-2014-2828	Medium		The V3 API in OpenStack Identity (Keystone) 2013.1 before 2013.2.4 and icehouse before icehouse-rc2 allows remote attackers to cause a denial of service (CPU consumption) via a large number of the same authentication method in a request, aka authentication chaining.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1838
7352	CVE-2014-2739	Medium		The cma_req_handler function in drivers/infiniband/core/cma.c in the Linux kernel 3.14.x through 3.14.1 attempts to resolve an RDMA over Converged Ethernet (aka RoCE) address that is properly resolved within a different module, which allows remote attackers to cause a denial of service (incorrect pointer dereference and system crash) via crafted network traffic.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7274

	A	B	C	D	E	F	G	H	I	J	K	L	M
7353	CVE-2014-2734	Medium		The openssl extension in Ruby 2.x does not properly maintain the state of process memory after a file is reopened, which allows remote attackers to spoof signatures within the context of a Ruby script that attempts signature verification after performing a certain sequence of filesystem operations.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7260
7354	CVE-2014-2707	Medium		cups-browsed in cups-filters 1.0.41 before 1.0.51 in allows remote IPP printers to execute arbitrary commands via shell metacharacters in the (1) model or (2) PDL, related to System V interface scripts generated for queues.	cups	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7278
7355	CVE-2014-2706	High		Race condition in the mac80211 subsystem in the Linux kernel before 3.13.7 allows remote attackers to cause a denial of service (system crash) via network traffic that improperly interacts with the WLAN_STA_PS_STA state (aka power-save mode), related to sta_info.c and tx.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7291
7356	CVE-2014-2678	Medium		The rds_iw_laddr_check function in net/rds/iw.c in the Linux kernel through 3.14 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a bind system call for an RDS socket on a system that lacks RDS transports.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7121
7357	CVE-2014-2673	Medium		The arch_dup_task_struct function in the Transactional Memory (TM) implementation in arch/powerpc/kernel/process.c in the Linux kernel before 3.13.7 on the powerpc platform does not properly interact with the clone and fork system calls, which allows local users to cause a denial of service (Program Check and system crash) via certain instructions that are executed with the processor in the Transactional state.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7126
7358	CVE-2014-2672	High		Race condition in the ath_tx_aggr_sleep function in drivers/net/wireless/ath/ath9k/xmit.c in the Linux kernel before 3.13.7 allows remote attackers to cause a denial of service (system crash) via a large amount of network traffic that triggers certain list deletions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7132
7359	CVE-2014-2669	Medium		Multiple integer overflows in contrib/hstore/hstore_io.c in PostgreSQL 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to have unspecified impact via vectors related to the (1) hstore_recv, (2) hstore_from_arrays, and (3) hstore_from_array functions in contrib/hstore/hstore_io.c; and the (4) hstoreArrayToPairs function in contrib/hstore/hstore_op.c, which triggers a buffer overflow. NOTE: this issue was SPLIT from CVE-2014-0064 because it has a different set of affected versions.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7122
7360	CVE-2014-2667	LOW		Race condition in the _get_masked_mode function in Lib/os.py in Python 3.2 through 3.5, when exist_ok is set to true and multiple threads are used, might allow local users to bypass intended file permissions by leveraging a separate application vulnerability before the umask has been set to the expected value.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8762
7361	CVE-2014-2653	Medium		The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7028
7362	CVE-2014-2599	Medium		The HVMOP_set_mem_access HVM control operations in Xen 4.1.x for 32-bit and 4.1.x through 4.4.x for 64-bit allow local guest administrators to cause a denial of service (CPU consumption) by leveraging access to certain service domains for HVM guests and a large input.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1790
7363	CVE-2014-2583	Medium		Multiple directory traversal vulnerabilities in pam_timestamp.c in the pam_timestamp module for Linux-PAM (aka pam) 1.1.8 allow local users to create aribitrary files or possibly bypass authentication via a .. (dot dot) in the (1) PAM_RUSER value to the get_ruser function or (2) PAM_TTY value to the check_tty funtion, which is used by the format_timestamp_name function.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7119
7364	CVE-2014-2573	Low		The VMWare driver in OpenStack Compute (Nova) 2013.2 through 2013.2.2 does not properly put VMs into RESCUE status, which allows remote authenticated users to bypass the quota limit and cause a denial of service (resource consumption) by requesting the VM be put into rescue and then deleting the image.	openstak	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1755
7365	CVE-2014-2568	Low		Use-after-free vulnerability in the nfqnl_zcopy function in net/netfilter/nfnetlink_queue_core.c in the Linux kernel through 3.13.6 allows attackers to obtain sensitive information from kernel memory by leveraging the absence of a certain orphaning operation. NOTE: the affected code was moved to the skb_zerocopy function in net/core/skbuff.c before the vulnerability was announced.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7033
7366	CVE-2014-2532	Medium		sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7031
7367	CVE-2014-2525	Medium		Heap-based buffer overflow in the yaml_parser_scan_uri_escapes function in LibYAML before 0.1.6 allows context-dependent attackers to execute arbitrary code via a long sequence of percent-encoded characters in a URI in a YAML file.	libyaml	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7131
7368	CVE-2014-2524	Low		The _rl_tropen function in util.c in GNU readline before 6.3 patch 3 allows local users to create or overwrite arbitrary files via a symlink attack on a /var/tmp/rltrace.[PID] file.	readline	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8281

	A	B	C	D	E	F	G	H	I	J	K	L	M
7369	CVE-2014-2523	High		net/netfilter/nf_conntrack_proto_dccp.c in the Linux kernel through 3.13.6 uses a DCCP header pointer incorrectly, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a DCCP packet that triggers a call to the (1) dccp_new, (2) dccp_packet, or (3) dccp_error function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7020
7370	CVE-2014-2497	Medium		The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7030
7371	CVE-2014-2494	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.37 and earlier allows remote authenticated users to affect availability via vectors related to ENARC.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8077
7372	CVE-2014-2484	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to SRFTS.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8089
7373	CVE-2014-2451	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7264
7374	CVE-2014-2450	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7277
7375	CVE-2014-2444	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7269
7376	CVE-2014-2442	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via vectors related to MyISAM.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7286
7377	CVE-2014-2440	Medium		Unspecified vulnerability in the MySQL Client component in Oracle MySQL 5.5.36 and earlier and 5.6.16 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7282
7378	CVE-2014-2438	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.35 and earlier and 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7284
7379	CVE-2014-2436	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.36 and earlier and 5.6.16 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to RBR.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7273
7380	CVE-2014-2435	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.16 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7275
7381	CVE-2014-2434	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via vectors related to DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7262
7382	CVE-2014-2432	Low		Unspecified vulnerability Oracle the MySQL Server component 5.5.35 and earlier and 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Federated.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7287
7383	CVE-2014-2431	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.36 and earlier and 5.6.16 and earlier allows remote attackers to affect availability via unknown vectors related to Options.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7272
7384	CVE-2014-2430	Low		Unspecified vulnerability in Oracle MySQL Server 5.5.36 and earlier and 5.6.16 and earlier allows remote authenticated users to affect availability via unknown vectors related to Performance Schema.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7293
7385	CVE-2014-2419	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.35 and earlier and 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7266
7386	CVE-2014-2405	High		Unspecified vulnerability in OpenJDK 6 before 6b31 on Debian GNU/Linux and Ubuntu 12.04 LTS and 10.04 LTS has unknown impact and attack vectors, a different vulnerability than CVE-2014-0462.	openjdk	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1869
7387	CVE-2014-2338	Medium		IKEv2 in strongSwan 4.0.7 before 5.1.3 allows remote attackers to bypass authentication by rekeying an IKE_SA during (1) initiation or (2) re-authentication, which triggers the IKE_SA state to be set to established.	strongswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7289
7388	CVE-2014-2324	Medium		Multiple directory traversal vulnerabilities in (1) mod_evhost and (2) mod_simple_vhost in lighttpd before 1.4.35 allow remote attackers to read arbitrary files via a .. (dot dot) in the host name, related to request_check_hostname.	lighttpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7035
7389	CVE-2014-2323	High		SQL injection vulnerability in mod_mysql_vhost.c in lighttpd before 1.4.35 allows remote attackers to execute arbitrary SQL commands via the host name, related to request_check_hostname.	lighttpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7025
7390	CVE-2014-2310	Medium		The AgentX subagent in Net-SNMP before 5.4.4 allows remote attackers to cause a denial of service (hang) by sending a multi-object request with an Object ID (OID) containing more subids than previous requests, a different vulnerability than CVE-2012-6151.	net-snmp	Unchanged	Vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	CGP6-443
7391	CVE-2014-2309	Medium		The ip6_route_add function in net/ipv6/route.c in the Linux kernel through 3.13.6 does not properly count the addition of routes, which allows remote attackers to cause a denial of service (memory consumption) via a flood of ICMPv6 Router Advertisement packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6968

	A	B	C	D	E	F	G	H	I	J	K	L	M
7392	CVE-2014-2285	Medium		The perl_trapd_handler function in perl/TrapReceiver/TrapReceiver.xs in Net-SNMP 5.7.3.pre3 and earlier, when using certain Perl versions, allows remote attackers to cause a denial of service (snmptrapd crash) via an empty community string in an SNMP trap, which triggers a NULL pointer dereference within the newSVpv function in Perl.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	CGP6-444
7393	CVE-2014-2284	Medium		The Linux implementation of the ICMP-MIB in Net-SNMP 5.5 before 5.5.2.1, 5.6.x before 5.6.2.1, and 5.7.x before 5.7.2.1 does not properly validate input, which allows remote attackers to cause a denial of service via unspecified vectors.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	CGP6-432
7394	CVE-2014-2263	High		The mpegts_write_pmt function in the MPEG2 transport stream (aka DVB) muxer (libavformat/mpegtsenc.c) in FFmpeg, possibly 2.1 and earlier, allows remote attackers to have unspecified impact and vectors, which trigger an out-of-bounds write.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6970
7395	CVE-2014-2241	Medium		The (1) cf2_initLocalRegionBuffer and (2) cf2_initGlobalRegionBuffer functions in cff/cf2ft.c in FreeType before 2.5.3 do not properly check if a subroutine exists, which allows remote attackers to cause a denial of service (assertion failure), as demonstrated by a crafted ttf file.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7029
7396	CVE-2014-2240	High		Stack-based buffer overflow in the cf2_hintmap_build function in cff/cf2hints.c in FreeType before 2.5.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large number of stem hints in a font file.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7024
7397	CVE-2014-2237	Medium		The memcache token backend in OpenStack Identity (Keystone) 2013.1 through 2.013.1.4, 2013.2 through 2013.2.2, and Icehouse before icehouse-3, when issuing a trust token with impersonation enabled, does not include this token in the trustee's token-index-list, which prevents the token from being invalidated by bulk token revocation and allows the trustee to bypass intended access restrictions.	opestack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1791
7398	CVE-2014-2099	Medium		The msrle_decode_frame function in libavcodec/msrle.c in FFmpeg before 2.1.4 does not properly calculate line sizes, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Microsoft RLE video data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6964
7399	CVE-2014-2098	Medium		libavcodec/wmalosslessdec.c in FFmpeg before 2.1.4 uses an incorrect data-structure size for certain coefficients, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted WMA data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6961
7400	CVE-2014-2097	Medium		The tak_decode_frame function in libavcodec/takdec.c in FFmpeg before 2.1.4 does not properly validate a certain bits-per-sample value, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted TAK (aka Tom's lossless Audio Kompressor) data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6967
7401	CVE-2014-2039	Medium		arch/s390/kernel/head64.S in the Linux kernel before 3.13.5 on the s390 platform does not properly handle attempted use of the linkage stack, which allows local users to cause a denial of service (system crash) by executing a crafted instruction.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6856
7402	CVE-2014-2038	Low		The nfs_can_extend_write function in fs/nfs/write.c in the Linux kernel before 3.13.3 relies on a write delegation to extend a write operation without a certain up-to-date verification, which allows local users to obtain sensitive information from kernel memory in opportunistic circumstances by writing to a file in an NFS filesystem and then reading the same file.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6875
7403	CVE-2014-2020	Medium		ext/gd/gd.c in PHP 5.5.x before 5.5.9 does not check data types, which might allow remote attackers to obtain sensitive information by using a (1) string or (2) array data type in place of a numeric data type, as demonstrated by an imagecrop function call with a string for the x dimension value, a different vulnerability than CVE-2013-7226.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6884
7404	CVE-2014-2015	High		Stack-based buffer overflow in the normify function in the rlm_pap module (modules/rlm_pap/rlm_pap.c) in FreeRADIUS 2.x, possibly 2.2.3 and earlier, and 3.x, possibly 3.0.1 and earlier, might allow attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long password hash, as demonstrated by an SSHA hash.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2123
7405	CVE-2014-1959	Medium		lib/x509/verify.c in GnuTLS before 3.1.21 and 3.2.x before 3.2.11 treats version 1 X.509 certificates as intermediate CAs, which allows remote attackers to bypass intended restrictions by leveraging a X.509 V1 certificate from a trusted CA to issue new certificates.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6962
7406	CVE-2014-1950	Medium		Use-after-free vulnerability in the xc_cpupool_getinfo function in Xen 4.1.x through 4.3.x, when using a multithreaded toolstack, does not properly handle a failure by the xc_cpumap_alloc function, which allows local users with access to management functions to cause a denial of service (heap corruption) and possibly gain privileges via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1707
7407	CVE-2014-1949	High		GTK+ 3.10.9 and earlier, as used in cinnamon-screensaver, gnome-screensaver, and other applications, allows physically proximate attackers to bypass the lock screen by pressing the menu button.	gtk+	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-140
7408	CVE-2014-1948	Low		OpenStack Image Registry and Delivery Service (Glance) 2013.2 through 2013.2.1 and Icehouse before icehouse-2 logs a URL containing the Swift store backend password when authentication fails and WARNING level logging is enabled, which allows local users to obtain sensitive information by reading the log.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1708

	A	B	C	D	E	F	G	H	I	J	K	L	M
7409	CVE-2014-1912	High		Buffer overflow in the socket.recvfrom_into function in Modules/socketmodule.c in Python 2.5 before 2.7.7, 3.x before 3.3.4, and 3.4.x before 3.4rc1 allows remote attackers to execute arbitrary code via a crafted string.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6966
7410	CVE-2014-1896	Medium		The (1) do_send and (2) do_recv functions in io.c in libvchan in Xen 4.2.x, 4.3.x, and 4.4-RC series allows local guests to cause a denial of service or possibly gain privileges via crafted xenstore ring indexes, which triggers a read or write past the end of the ring.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1789
7411	CVE-2014-1895	Medium		Off-by-one error in the flask_security_avc_cachestats function in xsm/flask/flask_op.c in Xen 4.2.x and 4.3.x, when the maximum number of physical CPUs are in use, allows local users to cause a denial of service (host crash) or obtain sensitive information from hypervisor memory by leveraging a FLASK_AVC_CACHESTAT hypercall, which triggers a buffer over-read.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1792
7412	CVE-2014-1893	Medium		Multiple integer overflows in the (1) FLASK_GETBOOL and (2) FLASK_SETBOOL suboperations in the flask hypercall in Xen 4.1.x, 3.3.x, 3.2.x, and earlier, when XSM is enabled, allow local users to cause a denial of service (processor fault) via unspecified vectors, a different vulnerability than CVE-2014-1891, CVE-2014-1892, and CVE-2014-1894.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1786
7413	CVE-2014-1892	Medium		Xen 3.3 through 4.1, when XSM is enabled, allows local users to cause a denial of service via vectors related to a large memory allocation, a different vulnerability than CVE-2014-1891, CVE-2014-1893, and CVE-2014-1894.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1794
7414	CVE-2014-1891	Medium		Multiple integer overflows in the (1) FLASK_GETBOOL, (2) FLASK_SETBOOL, (3) FLASK_USER, and (4) FLASK_CONTEXT_TO_SID suboperations in the flask hypercall in Xen 4.3.x, 4.2.x, 4.1.x, 3.2.x, and earlier, when XSM is enabled, allow local users to cause a denial of service (processor fault) via unspecified vectors, a different vulnerability than CVE-2014-1892, CVE-2014-1893, and CVE-2014-1894.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1793
7415	CVE-2014-1879	Low		Cross-site scripting (XSS) vulnerability in import.php in phpMyAdmin before 4.1.7 allows remote authenticated users to inject arbitrary web script or HTML via a crafted filename in an import action.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6858
7416	CVE-2014-1876	Low		The unpacker::redirect_stdio function in unpack.cpp in unpack200 in OpenJDK 6, 7, and 8, and Oracle Java JDK, does not securely create temporary files when a log file cannot be opened, which allows local users to overwrite arbitrary files via a symlink attack on /tmp/unpack.log.	openjdk	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1664
7417	CVE-2014-1874	Medium		The security_context_to_sid_core function in security/selinux/ss/services.c in the Linux kernel before 3.13.4 allows local users to cause a denial of service (system crash) by leveraging the CAP_MAC_ADMIN capability to set a zero-length security context.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6852
7418	CVE-2014-1859			(1) core/tests/test_memmap.py, (2) core/tests/test_multiarray.py, (3) f2py/f2py2e.py, and (4) lib/tests/test_io.py in NumPy before 1.8.1 allow local users to write to arbitrary files via a symlink attack on a temporary file.	python-numpy	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3103
7419	CVE-2014-1858			__init__.py in f2py in NumPy before 1.8.1 allows local users to write to arbitrary files via a symlink attack on a temporary file.	python-numpy	Unchanged	8.0.0.25	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3081
7420	CVE-2014-1739	Low		The media_device_enum_entities function in drivers/media/media-device.c in the Linux kernel before 3.14.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory by leveraging /dev/media0 read access for a MEDIA_IOC_ENUM_ENTITIES ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7789
7421	CVE-2014-1738	Medium		The raw_cmd_copyout function in drivers/block/floppy.c in the Linux kernel through 3.14.3 does not properly restrict access to certain pointers during processing of an FDRAWCMD ioctl call, which allows local users to obtain sensitive information from kernel heap memory by leveraging write access to a /dev/fd device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7435
7422	CVE-2014-1737	High		The raw_cmd_copyin function in drivers/block/floppy.c in the Linux kernel through 3.14.3 does not properly handle error conditions during processing of an FDRAWCMD ioctl call, which allows local users to trigger kfree operations and gain privileges by leveraging write access to a /dev/fd device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7419
7423	CVE-2014-1692	High		The hash_buffer function in schnorr.c in OpenSSH through 6.4, when Makefile.inc is modified to enable the J-PAKE protocol, does not initialize certain data structures, which might allow remote attackers to cause a denial of service (memory corruption) or have unspecified other impact via vectors that trigger an error condition.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6715
7424	CVE-2014-1690	Low		The help function in net/netfilter/nf_nat_irc.c in the Linux kernel before 3.12.8 allows remote attackers to obtain sensitive information from kernel memory by establishing an IRC DCC session in which incorrect packet data is transmitted during use of the NAT mangle feature.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6877
7425	CVE-2014-1666	High		The do_physdev_op function in Xen 4.1.5, 4.1.6.1, 4.2.2 through 4.2.3, and 4.3.x does not properly restrict access to the (1) PHYSDEVOP_prepare_msix and (2) PHYSDEVOP_release_msix operations, which allows local PV guests to cause a denial of service (host or guest malfunction) or possibly gain privileges via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1672

	A	B	C	D	E	F	G	H	I	J	K	L	M
7426	CVE-2014-1642	Medium		The IRQ setup in Xen 4.2.x and 4.3.x, when using device passthrough and configured to support a large number of CPUs, frees certain memory that may still be intended for use, which allows local guest administrators to cause a denial of service (memory corruption and hypervisor crash) and possibly execute arbitrary code via vectors related to an out-of-memory error that triggers a (1) use-after-free or (2) double free.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1674
7427	CVE-2014-1569	High		The definite_length_decoder function in lib/util/quickder.c in Mozilla Network Security Services (NSS) before 3.16.2.4 and 3.17.x before 3.17.3 does not ensure that the DER encoding of an ASN.1 length is properly formed, which allows remote attackers to conduct data-smuggling attacks by using a long byte sequence for an encoding, as demonstrated by the SEC_QuickDERDecodeItem function's improper handling of an arbitrary-length encoding of 0x00.CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2572
7428	CVE-2014-1568	High		Mozilla Network Security Services (NSS) before 3.16.2.1, 3.16.x before 3.16.5, and 3.17.x before 3.17.1, as used in Mozilla Firefox before 32.0.3, Mozilla Firefox ESR 24.x before 24.8.1 and 31.x before 31.1.1, Mozilla Thunderbird before 24.8.1 and 31.x before 31.1.2, Mozilla SeaMonkey before 2.29.1, Google Chrome before 37.0.2062.124 on Windows and OS X, and Google Chrome OS before 37.0.2062.120, does not properly parse ASN.1 values in X.509 certificates, which makes it easier for remote attackers to spoof RSA signatures via a crafted certificate, aka a signature malleability issue.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8564
7429	CVE-2014-1545	High		Mozilla Netscape Portable Runtime (NSPR) before 4.10.6 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write) via vectors involving the sprintf and console functions.Per: http://cwe.mitre.org/data/definitions/787.html CWE-787: Out-of-bounds Write	nspr	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7671
7430	CVE-2014-1544	High		Use-after-free vulnerability in the CERT_DestroyCertificate function in libnss3.so in Mozilla Network Security Services (NSS) 3.x, as used in Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7, allows remote attackers to execute arbitrary code via vectors that trigger certain improper removal of an NSSCertificate structure from a trust domain.CWE-416: Use After Free	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8087
7431	CVE-2014-1492	Medium		The cert_TestHostName function in lib/certdb/certdb.c in the certificate-checking implementation in Mozilla Network Security Services (NSS) before 3.16 accepts a wildcard character that is embedded in an internationalized domain name's U-label, which might allow man-in-the-middle attackers to spoof SSL servers via a crafted certificate.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	CGP6-433
7432	CVE-2014-1447	Low		Race condition in the virNetServerClientStartKeepAlive function in libvirt before 1.2.1 allows remote attackers to cause a denial of service (libvirtd crash) by closing a connection before a keepalive response is sent.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6759
7433	CVE-2014-1446	Low		The yam_ioctl function in drivers/net/hamradio/yam.c in the Linux kernel before 3.12.8 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability for an SIOCYAMGCFG ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6787
7434	CVE-2014-1445	Low		The wanxl_ioctl function in drivers/net/wan/wanxl.c in the Linux kernel before 3.11.7 does not properly initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory via an ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6767
7435	CVE-2014-1444	Low		The fst_get_iface function in drivers/net/wan/farsync.c in the Linux kernel before 3.11.7 does not properly initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability for an SIOCWANDEV ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6729
7436	CVE-2014-1438	Medium		The restore_fpu_checking function in arch/x86/include/asm/fpu-internal.h in the Linux kernel before 3.12.8 on the AMD K7 and K8 platforms does not clear pending exceptions before proceeding to an EMMS instruction, which allows local users to cause a denial of service (task kill) or possibly gain privileges via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6736
7437	CVE-2014-1270	Medium		WebKit, as used in Apple Safari before 6.1.2 and 7.x before 7.0.2, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than CVE-2014-1268 and CVE-2014-1269.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6857
7438	CVE-2014-1234	Low		The paratrooper-newrelic gem 1.0.1 for Ruby allows local users to obtain the X-Api-Key value by listing the curl process.	Ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6585
7439	CVE-2014-10072			In utils.c in zsh before 5.0.6, there is a buffer overflow when scanning very long directory paths for symbolic links.	zsh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	LIN10-3507
7440	CVE-2014-10071			In exec.c in zsh before 5.0.7, there is a buffer overflow for very long fds in the >& fd syntax.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3578

	A	B	C	D	E	F	G	H	I	J	K	L	M
7441	CVE-2014-10070			zsh before 5.0.7 allows evaluation of the initial values of integer variables imported from the environment (instead of treating them as literal numbers). That could allow local privilege escalation, under some specific and atypical conditions where zsh is being invoked in privilege-elevation contexts when the environment has not been properly sanitized, such as when zsh is invoked by sudo on systems where env_reset has been disabled.	zsh	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN10-3572
7442	CVE-2014-0591	Low		The query_findclosestnsec3 function in query.c in named in ISC BIND 9.6, 9.7, and 9.8 before 9.8.6-P2 and 9.9 before 9.9.4-P2, and 9.6-ESV before 9.6-ESV-R10-P2, allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via a crafted DNS query to an authoritative nameserver that uses the NSEC3 signing feature.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6749
7443	CVE-2014-0490	High		The apt-get download command in APT before 1.0.9 does not properly validate signatures for packages, which allows remote attackers to execute arbitrary code via a crafted package.	apt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2165
7444	CVE-2014-0489	High		APT before 1.0.9, when the Acquire::GzipIndexes option is enabled, does not validate checksums, which allows remote attackers to execute arbitrary code via a crafted package.	apt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2103
7445	CVE-2014-0488	Medium		APT before 1.0.9 does not invalidate repository data when moving from an unauthenticated to authenticated state, which allows remote attackers to have unspecified impact via crafted repository data.	apt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2137
7446	CVE-2014-0487	High		APT before 1.0.9 does not verify downloaded files if they have been modified as indicated using the If-Modified-Since header, which has unspecified impact and attack vectors.	apt	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2163
7447	CVE-2014-0478	Medium		APT before 1.0.4 does not properly validate source packages, which allows man-in-the-middle attackers to download and install Trojan horse packages by removing the Release signature.	apt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7793
7448	CVE-2014-0475	Medium		Multiple directory traversal vulnerabilities in GNU C Library (aka glibc or libc6) before 2.20 allow context-dependent attackers to bypass ForceCommand restrictions and possibly have other unspecified impact via a .. (dot dot) in a (1) LC_*, (2) LANG, or other locale environment variable.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8081
7449	CVE-2014-0471	High		Directory traversal vulnerability in the unpacking functionality in dpkg before 1.15.9, 1.16.x before 1.16.13, and 1.17.x before 1.17.8 allows remote attackers to write arbitrary files via a crafted source package, related to C-style filename quoting.	dpkg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7425
7450	CVE-2014-0462	High		Unspecified vulnerability in OpenJDK 6 before 6b31 on Debian GNU/Linux and Ubuntu 12.04 LTS and 10.04 LTS has unknown impact and attack vectors, a different vulnerability than CVE-2014-2405.	openjdk	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1872
7451	CVE-2014-0437	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6719
7452	CVE-2014-0433	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote attackers to affect availability via unknown vectors related to Thread Pooling.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6760
7453	CVE-2014-0431	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-5881.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6743
7454	CVE-2014-0430	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Performance Schema.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6727
7455	CVE-2014-0427	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via vectors related to FTS.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6744
7456	CVE-2014-0420	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.34 and earlier, and 5.6.14 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6780
7457	CVE-2014-0412	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6740
7458	CVE-2014-0402	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Locking.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6773
7459	CVE-2014-0401	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6714
7460	CVE-2014-0393	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier allows remote authenticated users to affect integrity via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6732
7461	CVE-2014-0386	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6777

	A	B	C	D	E	F	G	H	I	J	K	L	M
7462	CVE-2014-0384	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.35 and earlier and 5.6.15 and earlier allows remote authenticated users to affect availability via vectors related to XML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7263
7463	CVE-2014-0333	Medium		The png_push_read_chunk function in pngpread.c in the progressive decoder in libpng 1.6.x through 1.6.9 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via an IDAT chunk with a length of zero.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6865
7464	CVE-2014-0246	Medium		SOSreport stores the md5 hash of the GRUB bootloader password in an archive, which allows local users to obtain sensitive information by reading the archive.	grub	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7576
7465	CVE-2014-0244	Low		The sys_recvfrom function in nmbd in Samba 3.6.x before 3.6.24, 4.0.x before 4.0.19, and 4.1.x before 4.1.9 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a malformed UDP packet.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7795
7466	CVE-2014-0239	Medium		The internal DNS server in Samba 4.x before 4.0.18 does not check the QR field in the header section of an incoming DNS message before sending a response, which allows remote attackers to cause a denial of service (CPU and bandwidth consumption) via a forged response packet that triggers a communication loop, a related issue to CVE-1999-0103.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7580
7467	CVE-2014-0238	Medium		The cdf_read_property_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7676
7468	CVE-2014-0237	Medium		The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7665
7469	CVE-2014-0236	Medium		file before 5.18, as used in the Fileinfo component in PHP before 5.6.0, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a zero root_storage value in a CDF file, related to cdf.c and readcdf.c.CWE-476: NULL Pointer Dereference	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-762
7470	CVE-2014-0231	Medium		The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8082
7471	CVE-2014-0226	Medium		Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8067
7472	CVE-2014-0224	Medium		OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the CCS Injection vulnerability.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7632
7473	CVE-2014-0223	Medium		Integer overflow in the qcow_open function in block/qcow.c in QEMU before 1.7.2 allows local users to cause a denial of service (crash) and possibly execute arbitrary code via a large image size, which triggers a buffer overflow or out-of-bounds read.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2122
7474	CVE-2014-0222	High		Integer overflow in the qcow_open function in block/qcow.c in QEMU before 1.7.2 allows remote attackers to cause a denial of service (crash) via a large L2 table in a QCOW version 1 image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2170
7475	CVE-2014-0221	Medium		The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7629
7476	CVE-2014-0211	High		Multiple integer overflows in the (1) fs_get_reply, (2) fs_alloc_glyphs, and (3) fs_read_extent_info functions in X.Org libXfont before 1.4.8 and 1.4.9x before 1.4.99.901 allow remote font servers to execute arbitrary code via a crafted xfs reply, which triggers a buffer overflow.	libxfont	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7583
7477	CVE-2014-0210	High		Multiple buffer overflows in X.Org libXfont before 1.4.8 and 1.4.9x before 1.4.99.901 allow remote font servers to execute arbitrary code via a crafted xfs protocol reply to the (1) _fs_recv_conn_setup, (2) fs_read_open_font, (3) fs_read_query_info, (4) fs_read_extent_info, (5) fs_read_glyphs, (6) fs_read_list, or (7) fs_read_list_info function.	libxfont	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7579
7478	CVE-2014-0209	Medium		Multiple integer overflows in the (1) FontFileAddEntry and (2) lexAlias functions in X.Org libXfont before 1.4.8 and 1.4.9x before 1.4.99.901 might allow local users to gain privileges by adding a directory with a large fonts.dir or fonts.alias file to the font path, which triggers a heap-based buffer overflow, related to metadata.	libxfont	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7584
7479	CVE-2014-0207	Medium		The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted CDF file.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7950

	A	B	C	D	E	F	G	H	I	J	K	L	M
7480	CVE-2014-0206	Low		Array index error in the aio_read_events_ring function in fs/aio.c in the Linux kernel through 3.15.1 allows local users to obtain sensitive information from kernel memory via a large head value.Per: http://cwe.mitre.org/data/definitions/129.html CWE-129: Improper Validation of Array Index	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7791
7481	CVE-2014-0205	Medium		The futex_wait function in kernel/futex.c in the Linux kernel before 2.6.37 does not properly maintain a certain reference count during requeue operations, which allows local users to cause a denial of service (use-after-free and system crash) or possibly gain privileges via a crafted application that triggers a zero count.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8550
7482	CVE-2014-0203	Medium		The __do_follow_link function in fs/namei.c in the Linux kernel before 2.6.33 does not properly handle the last pathname component during use of certain filesystems, which allows local users to cause a denial of service (incorrect free operations and system crash) via an open system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7792
7483	CVE-2014-0198	Medium		The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7429
7484	CVE-2014-0196	Medium		The n_tty_write function in drivers/tty/n_tty.c in the Linux kernel through 3.14.3 does not properly manage tty driver access in the LECHO & !OPOST case, which allows local users to cause a denial of service (memory corruption and system crash) or gain privileges by triggering a race condition involving read and write operations with long strings.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7413
7485	CVE-2014-0195	Medium		The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7627
7486	CVE-2014-0191	Medium		The xmlParserHandlePEReference function in parser.c in libxml2 before 2.9.2, as used in Web Listener in Oracle HTTP Server in Oracle Fusion Middleware 11.1.1.7.0, 12.1.2.0, and 12.1.3.0 and other products, loads external parameter entities regardless of whether entity substitution or validation is enabled, which allows remote attackers to cause a denial of service (resource consumption) via a crafted XML document.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2759
7487	CVE-2014-0190	Medium		The GIF decoder in QtGui in Qt before 5.3 allows remote attackers to cause a denial of service (NULL pointer dereference) via invalid width and height values in a GIF image.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7416
7488	CVE-2014-0187	High		The openvswitch-agent process in OpenStack Neutron 2013.1 before 2013.2.4 and 2014.1 before 2014.1.1 allows remote authenticated users to bypass security group restrictions via an invalid CIDR in a security group rule, which prevents further rules from being applied.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1867
7489	CVE-2014-0185	High		sapi/fpm/fpm/fpm_unix.c in the FastCGI Process Manager (FPM) in PHP before 5.4.28 and 5.5.x before 5.5.12 uses 0666 permissions for the UNIX socket, which allows local users to gain privileges via a crafted FastCGI client.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7418
7490	CVE-2014-0182	High		Heap-based buffer overflow in the virtio_load function in hw/virtio/virtio.c in QEMU before 1.7.2 might allow remote attackers to execute arbitrary code via a crafted config length in a savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2136
7491	CVE-2014-0181	Low		The Netlink implementation in the Linux kernel through 3.14.1 does not provide a mechanism for authorizing socket operations based on the opener of a socket, which allows local users to bypass intended access restrictions and modify network configurations by using a Netlink socket for the (1) stdout or (2) stderr of a setuid program.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7270
7492	CVE-2014-0179	Low		libvirt 0.7.5 through 1.2.x before 1.2.5 allows local users to cause a denial of service (read block and hang) via a crafted XML document containing an XML external entity declaration in conjunction with an entity reference to the (1) virConnectCompareCPU or (2) virConnectBaselineCPU API method, related to an XML External Entity (XXE) issue. NOTE: this issue was SPLIT per ADT3 due to different affected versions of some vectors. CVE-2014-5177 is used for other API methods.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8183
7493	CVE-2014-0178	Low		Samba 3.6.6 through 3.6.23, 4.0.x before 4.0.18, and 4.1.x before 4.1.8, when a certain vfs shadow copy configuration is enabled, does not properly initialize the SRV_SNAPSHOT_ARRAY response field, which allows remote authenticated users to obtain potentially sensitive information from process memory via a (1) FSCTL_GET_SHADOW_COPY_DATA or (2) FSCTL_SRV_ENUMERATE_SNAPSHOTS request.Per: http://cwe.mitre.org/data/definitions/665.html CWE-665: Improper Initialization	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7577
7494	CVE-2014-0167	Medium		The Nova EC2 API security group implementation in OpenStack Compute (Nova) 2013.1 before 2013.2.4 and icehouse before icehouse-rc2 does not enforce RBAC policies for (1) add_rules, (2) remove_rules, (3) destroy, and other unspecified methods in compute/api.py when using non-default policies, which allows remote authenticated users to gain privileges via these API requests.	openstack compute	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1833

	A	B	C	D	E	F	G	H	I	J	K	L	M
7495	CVE-2014-0162	Medium		The Sheepdog backend in OpenStack Image Registry and Delivery Service (Glance) 2013.2 before 2013.2.4 and icehouse before icehouse-rc2 allows remote authenticated users with permission to insert or modify an image to execute arbitrary commands via a crafted location.	openstack icehouse	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1835
7496	CVE-2014-0160	Medium		The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7088
7497	CVE-2014-0157	Medium		Cross-site scripting (XSS) vulnerability in the Horizon Orchestration dashboard in OpenStack Dashboard (aka Horizon) 2013.2 before 2013.2.4 and icehouse before icehouse-rc2 allows remote attackers to inject arbitrary web script or HTML via the description field of a Heat template.	openstack horizon	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1834
7498	CVE-2014-0155	Medium		The ioapic_deliver function in virt/kvm/ioapic.c in the Linux kernel through 3.14.1 does not properly validate the kvm_irq_delivery_to_apic return value, which allows guest OS users to cause a denial of service (host OS crash) via a crafted entry in the redirection table of an I/O APIC. NOTE: the affected code was moved to the ioapic_service function before the vulnerability was announced.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7271
7499	CVE-2014-0154	Medium		oVirt Engine before 3.5.0 does not include the HTTPOnly flag in a Set-Cookie header for the session IDs, which makes it easier for remote attackers to obtain potentially sensitive information via script access to this cookie.	ovirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2318
7500	CVE-2014-0153	Medium		The REST API in oVirt 3.4.0 and earlier stores session IDs in HTML5 local storage, which allows remote attackers to obtain sensitive information via a crafted web page.	ovirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2093
7501	CVE-2014-0152	Medium		Session fixation vulnerability in the web admin interface in oVirt 3.4.0 and earlier allows remote attackers to hijack web sessions via unspecified vectors.	ovirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2091
7502	CVE-2014-0151	Medium		Cross-site request forgery (CSRF) vulnerability in oVirt Engine before 3.5.0 beta2 allows remote attackers to hijack the authentication of users for requests that perform unspecified actions via a REST API request.	ovirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-2320
7503	CVE-2014-0150	Medium		Integer overflow in the virtio_net_handle_mac function in hw/net/virtio-net.c in QEMU 2.0 and earlier allows local guest users to execute arbitrary code via a MAC addresses table update request, which triggers a heap-based buffer overflow.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7285
7504	CVE-2014-0146			The qcow2_open function in the (block/qcow2.c) in QEMU before 1.7.2 and 2.x before 2.0.0 allows local users to cause a denial of service (NULL pointer dereference) via a crafted image which causes an error, related to the initialization of the snapshot_offset and nb_snapshots fields.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5043
7505	CVE-2014-0145			Multiple buffer overflows in QEMU before 1.7.2 and 2.x before 2.0.0, allow local users to cause a denial of service (crash) or possibly execute arbitrary code via a large (1) L1 table in the qcow2_snapshot_load_tmp in the QCOW 2 block driver (block/qcow2-snapshot.c) or (2) uncompressed chunk, (3) chunk length, or (4) number of sectors in the DMG block driver (block/dmg.c).	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4931
7506	CVE-2014-0143			Multiple integer overflows in the block drivers in QEMU, possibly before 2.0.0, allow local users to cause a denial of service (crash) via a crafted catalog size in (1) the parallels_open function in block/parallels.c or (2) bochs_open function in bochs.c, a large L1 table in the (3) qcow2_snapshot_load_tmp in qcow2-snapshot.c or (4) qcow2_grow_l1_table function in qcow2-cluster.c, (5) a large request in the bdrv_check_byte_request function in block.c and other block drivers, (6) crafted cluster indexes in the get_refcount function in qcow2-refcount.c, or (7) a large number of blocks in the cloop_open function in cloop.c, which trigger buffer overflows, memory corruption, large memory allocations and out-of-bounds read and writes.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4952
7507	CVE-2014-0142			QEMU, possibly before 2.0.0, allows local users to cause a denial of service (divide-by-zero error and crash) via a zero value in the (1) tracks field to the seek_to_sector function in block/parallels.c or (2) extent_size field in the bochs function in block/bochs.c.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5062
7508	CVE-2014-0139	Medium		cURL and libcurl 7.1 before 7.36.0, when using the OpenSSL, axtls, qsossl or gskit libraries for TLS, recognize a wildcard IP address in the subject's Common Name (CN) field of an X.509 certificate, which might allow man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7145
7509	CVE-2014-0138	Medium		The default configuration in cURL and libcurl 7.10.6 before 7.36.0 re-uses (1) SCP, (2) SFTP, (3) POP3, (4) POP3S, (5) IMAP, (6) IMAPS, (7) SMTP, (8) SMTPS, (9) LDAP, and (10) LDAPS connections, which might allow context-dependent attackers to connect as other users via a request, a similar issue to CVE-2014-0015.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7144
7510	CVE-2014-0134	Low		The instance rescue mode in OpenStack Compute (Nova) 2013.2 before 2013.2.3 and Icehouse before 2014.1, when using libvirt to spawn images and use_cow_images is set to false, allows remote authenticated users to read certain compute host files by overwriting an instance disk with a crafted image.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1866

	A	B	C	D	E	F	G	H	I	J	K	L	M
7511	CVE-2014-0131	Low		Use-after-free vulnerability in the skb_segment function in net/core/skbuff.c in the Linux kernel through 3.13.6 allows attackers to obtain sensitive information from kernel memory by leveraging the absence of a certain orphaning operation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7034
7512	CVE-2014-0128	Medium		Squid 3.1 before 3.3.12 and 3.4 before 3.4.4, when SSL-Bump is enabled, allows remote attackers to cause a denial of service (assertion failure) via a crafted range request, related to state management.	squid	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1787
7513	CVE-2014-0118	Medium		The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8063
7514	CVE-2014-0117	Medium		The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.Per vendor advisory http://httpd.apache.org/security/vulnerabilities_24.html A flaw was found in mod_proxy in httpd versions 2.4.6 to 2.4.9.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8093
7515	CVE-2014-0106	Medium		Sudo 1.6.9 before 1.8.5, when env_reset is disabled, does not properly check environment variables for the env_delete restriction, which allows local users with sudo permissions to bypass intended command restrictions via a crafted environment variable.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6960
7516	CVE-2014-0105	Medium		The auth_token middleware in the OpenStack Python client library for Keystone (aka python-keystoneclient) before 0.7.0 does not properly retrieve user tokens from memcache, which allows remote authenticated users to gain privileges in opportunistic circumstances via a large number of requests, related to an interaction between eventlet and python-memcached.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1831
7517	CVE-2014-0102	Medium		The keyring_detect_cycle_iterator function in security/keys/keyring.c in the Linux kernel through 3.13.6 does not properly determine whether keyrings are identical, which allows local users to cause a denial of service (OOPS) via crafted keyctl commands.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6963
7518	CVE-2014-0101	High		The sctp_sf_do_5_1D_ce function in net/sctp/sm_statefuns.c in the Linux kernel through 3.13.6 does not validate certain auth_enable and auth_capable fields before making a sctp_sf_authenticate call, which allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via an SCTP handshake with a modified INIT chunk and a crafted AUTH chunk before a COOKIE_ECHO chunk.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6969
7519	CVE-2014-0100	High		Race condition in the inet_frag_intern function in net/ipv4/inet_fragment.c in the Linux kernel through 3.13.6 allows remote attackers to cause a denial of service (use-after-free error) or possibly have unspecified other impact via a large series of fragmented ICMP Echo Request packets to a system with a heavy CPU load.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6957
7520	CVE-2014-0098	Medium		The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7027
7521	CVE-2014-0092	Medium		lib/x509/verify.c in GnuTLS before 3.1.22 and 3.2.x before 3.2.12 does not properly handle unspecified errors when verifying X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers via a crafted certificate.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6965
7522	CVE-2014-0077	Medium		drivers/vhost/net.c in the Linux kernel before 3.13.10, when mergeable buffers are disabled, does not properly validate packet lengths, which allows guest OS users to cause a denial of service (memory corruption and host OS crash) or possibly gain privileges on the host OS via crafted packets, related to the handle_rx and get_rx_bufs functions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7276
7523	CVE-2014-0076	Medium		The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7038
7524	CVE-2014-0071	Medium		PackStack in Red Hat OpenStack 4.0 does not enforce the default security groups when deployed to Neutron, which allows remote attackers to bypass intended access restrictions and make unauthorized connections.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1832
7525	CVE-2014-0069	Medium		The cifs_iovec_write function in fs/cifs/file.c in the Linux kernel through 3.13.5 does not properly handle uncached write operations that copy fewer than the requested number of bytes, which allows local users to obtain sensitive information from kernel memory, cause a denial of service (memory corruption and system crash), or possibly gain privileges via a writev system call with a crafted pointer.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6874
7526	CVE-2014-0067	Medium		The make check command for the test suites in PostgreSQL 9.3.3 and earlier does not properly invoke initdb to specify the authentication requirements for a database cluster to be used for the tests, which allows local users to gain privileges by leveraging access to this cluster.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7127

	A	B	C	D	E	F	G	H	I	J	K	L	M
7527	CVE-2014-0066	Medium		The chkpass extension in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 does not properly check the return value of the crypt library function, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via unspecified vectors.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7134
7528	CVE-2014-0065	Medium		Multiple buffer overflows in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to have unspecified impact and attack vectors, a different vulnerability than CVE-2014-0063.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7133
7529	CVE-2014-0064	Medium		Multiple integer overflows in the path_in and other unspecified functions in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to have unspecified impact and attack vectors, which trigger a buffer overflow. NOTE: this identifier has been SPLIT due to different affected versions; use CVE-2014-2669 for the hstore vector.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7129
7530	CVE-2014-0063	Medium		Multiple stack-based buffer overflows in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via vectors related to an incorrect MAXDATELEN constant and datetime values involving (1) intervals, (2) timestamps, or (3) timezones, a different vulnerability than CVE-2014-0065.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7125
7531	CVE-2014-0062	Medium		Race condition in the (1) CREATE INDEX and (2) unspecified ALTER TABLE commands in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allows remote authenticated users to create an unauthorized index or read portions of unauthorized tables by creating or deleting a table with the same name during the timing window.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7123
7532	CVE-2014-0061	Medium		The validator functions for the procedural languages (PLs) in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to gain privileges via a function that is (1) defined in another language or (2) not allowed to be directly called by the user due to permissions.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7130
7533	CVE-2014-0060	Medium		PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 does not properly enforce the ADMIN OPTION restriction, which allows remote authenticated members of a role to add or remove arbitrary users to that role by calling the SET ROLE command before the associated GRANT command.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7128
7534	CVE-2014-0056	Low		The l3-agent in OpenStack Neutron 2012.2 before 2013.2.3 does not check the tenant id when creating ports, which allows remote authenticated users to plug ports into the routers of arbitrary tenants via the device id in a port-create command.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1871
7535	CVE-2014-0055	Medium		The get_rx_bufs function in drivers/vhost/net.c in the vhost-net subsystem in the Linux kernel package before 2.6.32-431.11.2 on Red Hat Enterprise Linux (RHEL) 6 does not properly handle vhost_get_vq_desc errors, which allows guest OS users to cause a denial of service (host OS crash) via unspecified vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7022
7536	CVE-2014-0049	High		Buffer overflow in the complete_emulated_mmio function in arch/x86/kvm/x86.c in the Linux kernel before 3.13.6 allows guest OS users to execute arbitrary code on the host OS by leveraging a loop that triggers an invalid memory copy affecting certain cancel_work_item data.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6959
7537	CVE-2014-0047			Docker before 1.5 allows local users to have unspecified impact via vectors involving unsafe /tmp usage.	docker	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5518
7538	CVE-2014-0042	Medium		OpenStack Heat Templates (heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 4.0, sets gpgcheck to 0 for certain templates, which disables GPG signature checking on downloaded packages and allows man-in-the-middle attackers to install arbitrary packages via unspecified vectors.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1929
7539	CVE-2014-0041	Medium		OpenStack Heat Templates (heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 4.0, sets sslverify to false for certain Yum repositories, which disables SSL protection and allows man-in-the-middle attackers to prevent updates via unspecified vectors.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1932
7540	CVE-2014-0040	Medium		OpenStack Heat Templates (heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 4.0, uses an HTTP connection to download (1) packages and (2) signing keys from Yum repositories, which allows man-in-the-middle attackers to prevent updates via unspecified vectors.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1927
7541	CVE-2014-0038	Medium		The compat_sys_recvmmsg function in net/compat.c in the Linux kernel before 3.13.2, when CONFIG_X86_X32 is enabled, allows local users to gain privileges via a recvmmsg system call with a crafted timeout pointer parameter.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6779
7542	CVE-2014-0031	Medium		The (1) ListNetworkACL and (2) listNetworkACLLists APIs in Apache CloudStack before 4.2.1 allow remote authenticated users to list network ACLS for other users via a crafted request.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6716

	A	B	C	D	E	F	G	H	I	J	K	L	M
7543	CVE-2014-0028	Medium		libvirt 1.1.1 through 1.2.0 allows context-dependent attackers to bypass the domain:getattr and connect:search_domains restrictions in ACLs and obtain sensitive domain object information via a request to the (1) virConnectDomainEventRegister and (2) virConnectDomainEventRegisterAny functions in the event registration API.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6763
7544	CVE-2014-0017	Low		The RAND_bytes function in libssh before 0.6.3, when forking is enabled, does not properly reset the state of the OpenSSL pseudo-random number generator (PRNG), which causes the state to be shared between children processes and allows local users to obtain sensitive information by leveraging a pid collision.	libssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7019
7545	CVE-2014-0015	Medium		cURL and libcurl 7.10.6 through 7.34.0, when more than one authentication method is enabled, re-uses NTLM connections, which might allow context-dependent attackers to authenticate as other users via a request.	libcurl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6726
7546	CVE-2014-0006	Medium		The TempURL middleware in OpenStack Object Storage (Swift) 1.4.6 through 1.8.0, 1.9.0 through 1.10.0, and 1.11.0 allows remote attackers to obtain secret URLs by leveraging an object name and a timing side-channel attack.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1660
7547	CVE-2014-0001	High		Buffer overflow in client/mysql.cc in Oracle MySQL and MariaDB before 5.5.35 allows remote database servers to cause a denial of service (crash) and possibly execute arbitrary code via a long server version string.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6735
7548	CVE-2013-7470	High	MEDIUM	cipso_v4_validate in include/net/cipso_ipv4.h in the Linux kernel before 3.11.7, when CONFIG_NETLABEL is disabled, allows attackers to cause a denial of service (infinite loop and crash), as demonstrated by icmpsic, a different vulnerability than CVE-2013-0310.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4046
7549	CVE-2013-7459	High	Critical	Heap-based buffer overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py.	python-pycrypto	Unchanged	8.0.0.15	9.0.0.4	10.0.0.0	Won't Fix	Won't Fix	Won't Fix	LIN9-3427
7550	CVE-2013-7458	Low		linenoise, as used in Redis before 3.2.3, uses world-readable permissions for .rediscli_history, which allows local users to obtain sensitive information by reading the file.	redis	Unchanged	8.0.0.9	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-1428
7551	CVE-2013-7456	Medium		gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.1.1, as used in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7, allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted image that is mishandled by the imagescale function.	gd	Unchanged	8.0.0.9	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1365
7552	CVE-2013-7447	MEDIUM		Integer overflow in the gdk_cairo_set_source_pixbuf function in gdk/gdkcairo.c in GTK+ before 3.9.8, as used in eom, gnome-photos, eog, gambas3, thunar, pinpoint, and possibly other applications, allows remote attackers to cause a denial of service (crash) via a large image file, which triggers a large memory allocation.	gtk	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-303
7553	CVE-2013-7446	Medium		Use-after-free vulnerability in net/unix/af_unix.c in the Linux kernel before 4.3.3 allows local users to bypass intended AF_UNIX socket permissions or cause a denial of service (panic) via crafted epoll_ctl calls.CWE-416: Use After Free	linux	Unchanged	8.0.0.1	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-73
7554	CVE-2013-7445	High		The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated by JavaScript code that creates many CANVAS elements for rendering by Chrome or Firefox.	linux	Unchanged	Investigate	Investigate	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	SCP7-218
7555	CVE-2013-7443	Medium		Buffer overflow in the skip-scan optimization in SQLite 3.8.2 allows remote attackers to cause a denial of service (crash) via crafted SQL statements.	sqlite	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-720
7556	CVE-2013-7440	Medium		The ssl.match_hostname function in CPython (aka Python) before 2.7.9 and 3.x before 3.3.3 does not properly handle wildcards in hostnames, which might allow man-in-the-middle attackers to spoof servers via a crafted certificate.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-830
7557	CVE-2013-7439	High		Multiple off-by-one errors in the (1) MakeBigReq and (2) SetReqLen macros in include/X11/Xlibint.h in X11R6.x and libX11 before 1.6.0 allow remote attackers to have unspecified impact via a crafted request, which triggers a buffer overflow.	libx11	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-327
7558	CVE-2013-7424	MEDIUM		Affects glibc's getaddrinfo() function "when used with the AI_IDN flag", and if "glibc is compiled with libidn support".	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-434
7559	CVE-2013-7423	Medium		The send_dg function in resolv/res_send.c in GNU C Library (aka glibc or libc6) before 2.20 does not properly reuse file descriptors, which allows remote attackers to send DNS queries to unintended locations via a large number of request that trigger a call to the getaddrinfo function.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-201
7560	CVE-2013-7422	High		Integer underflow in regcomp.c in Perl before 5.20, as used in Apple OS X before 10.10.5 and other products, allows context-dependent attackers to execute arbitrary code or cause a denial of service (application crash) via a long digit string associated with an invalid backreference within a regular expression.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-787
7561	CVE-2013-7421	Low		The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bind system call for an AF_ALG socket with a module name in the salg_name field, a different vulnerability than CVE-2014-9644.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-215

	A	B	C	D	E	F	G	H	I	J	K	L	M
7562	CVE-2013-7393	Low		The daemonize.py module in Subversion 1.8.0 before 1.8.2 allows local users to gain privileges via a symlink attack on the pid file created for (1) svnwcsub.py or (2) irkerbridge.py when the --pidfile option is used. NOTE: this issue was SPLIT from CVE-2013-4262 based on different affected versions (ADT3).	subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8075
7563	CVE-2013-7354	Medium		Multiple integer overflows in libpng before 1.5.14rc03 allow remote attackers to cause a denial of service (crash) via a crafted image to the (1) png_set_sPLT or (2) png_set_text_2 function, which triggers a heap-based buffer overflow.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7434
7564	CVE-2013-7353	Medium		Integer overflow in the png_set_unknown_chunks function in libpng/pngset.c in libpng before 1.5.14beta08 allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a crafted image, which triggers a heap-based buffer overflow.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7421
7565	CVE-2013-7348	Medium		Double free vulnerability in the ioctx_alloc function in fs/aio.c in the Linux kernel before 3.12.4 allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via vectors involving an error condition in the aio_setup_ring function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7120
7566	CVE-2013-7339	Medium		The rds_ib_laddr_check function in net/rds/ib.c in the Linux kernel before 3.12.8 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a bind system call for an RDS socket on a system that lacks RDS transports.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7026
7567	CVE-2013-7338	High		Python before 3.3.4 RC1 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a file size value larger than the size of the zip file to the (1) ZipExtFile.read, (2) ZipExtFile.read(n), (3) ZipExtFile.readlines, (4) ZipFile.extract, or (5) ZipFile.extractall function.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7261
7568	CVE-2013-7336	Low		The qemuMigrationWaitForSpice function in qemu/qemu_migration.c in libvirt before 1.1.3 does not properly enter a monitor when performing seamless SPICE migration, which allows local users to cause a denial of service (NULL pointer dereference and libvirtd crash) by causing domblkstat to be called at the same time as the qemuMonitorGetSpiceMigrationStatus function.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7433
7569	CVE-2013-7328	Medium		Multiple integer signedness errors in the gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 allow remote attackers to cause a denial of service (application crash) or obtain sensitive information via an imagecrop function call with a negative value for the (1) x or (2) y dimension, a different vulnerability than CVE-2013-7226.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6864
7570	CVE-2013-7327	Medium		The gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 does not check return values, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via invalid imagecrop arguments that lead to use of a NULL pointer as a return value, a different vulnerability than CVE-2013-7226.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6873
7571	CVE-2013-7295	Medium		Tor before 0.2.4.20, when OpenSSL 1.x is used in conjunction with a certain HardwareAccel setting on Intel Sandy Bridge and Ivy Bridge platforms, does not properly generate random numbers for (1) relay identity keys and (2) hidden-service identity keys, which might make it easier for remote attackers to bypass cryptographic protection mechanisms via unspecified vectors.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6737
7572	CVE-2013-7281	Medium		The dgram_recvmsg function in net/ieee802154/dgram.c in the Linux kernel before 3.12.4 updates a certain length value without ensuring that an associated data structure has been initialized, which allows local users to obtain sensitive information from kernel stack memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6578
7573	CVE-2013-7271	Medium		The x25_recvmsg function in net/x25/af_x25.c in the Linux kernel before 3.12.4 updates a certain length value without ensuring that an associated data structure has been initialized, which allows local users to obtain sensitive information from kernel memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6576
7574	CVE-2013-7270	Medium		The packet_recvmsg function in net/packet/af_packet.c in the Linux kernel before 3.12.4 updates a certain length value before ensuring that an associated data structure has been initialized, which allows local users to obtain sensitive information from kernel memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6586
7575	CVE-2013-7269	Medium		The nr_recvmsg function in net/netrom/af_netrom.c in the Linux kernel before 3.12.4 updates a certain length value without ensuring that an associated data structure has been initialized, which allows local users to obtain sensitive information from kernel memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6581
7576	CVE-2013-7268	Medium		The ipx_recvmsg function in net/ipx/af_ipx.c in the Linux kernel before 3.12.4 updates a certain length value without ensuring that an associated data structure has been initialized, which allows local users to obtain sensitive information from kernel memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6589

	A	B	C	D	E	F	G	H	I	J	K	L	M
7577	CVE-2013-7267	Medium		The atalk_recvmsg function in net/appletalk/ddp.c in the Linux kernel before 3.12.4 updates a certain length value without ensuring that an associated data structure has been initialized, which allows local users to obtain sensitive information from kernel memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6584
7578	CVE-2013-7266	Medium		The mISDN_sock_recvmsg function in drivers/isdn/mISDN/socket.c in the Linux kernel before 3.12.4 does not ensure that a certain length value is consistent with the size of an associated data structure, which allows local users to obtain sensitive information from kernel memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6574
7579	CVE-2013-7265	Medium		The pn_recvmsg function in net/phonet/datagram.c in the Linux kernel before 3.12.4 updates a certain length value before ensuring that an associated data structure has been initialized, which allows local users to obtain sensitive information from kernel stack memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6590
7580	CVE-2013-7264	Medium		The l2tp_ip_recvmsg function in net/l2tp/l2tp_ip.c in the Linux kernel before 3.12.4 updates a certain length value before ensuring that an associated data structure has been initialized, which allows local users to obtain sensitive information from kernel stack memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6587
7581	CVE-2013-7263	Medium		The Linux kernel before 3.12.4 updates certain length values before ensuring that associated data structures have been initialized, which allows local users to obtain sensitive information from kernel stack memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call, related to net/ipv4/ping.c, net/ipv4/raw.c, net/ipv4/udp.c, net/ipv6/raw.c, and net/ipv6/udp.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6579
7582	CVE-2013-7226	Medium		Integer overflow in the gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an imagecrop function call with a large x dimension value, leading to a heap-based buffer overflow.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6863
7583	CVE-2013-7130	High		The i_create_images_and_backing (aka create_images_and_backing) method in libvirt driver in OpenStack Compute (Nova) Grizzly, Havana, and Icehouse, when using KVM live block migration, does not properly create all expected files, which allows attackers to obtain snapshot root disk contents of other users via ephemeral storage.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1663
7584	CVE-2013-7048	Low		OpenStack Compute (Nova) Grizzly 2013.1.4, Havana 2013.2.1, and earlier uses world-writable and world-readable permissions for the temporary directory used to store live snapshots, which allows local users to read and modify live snapshots.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1661
7585	CVE-2013-7040	Medium		Python 2.7 before 3.4 only uses the last eight bits of the prefix to randomize hash values, which causes it to compute hash values without restricting the ability to trigger hash collisions predictably and makes it easier for context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1150.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7582
7586	CVE-2013-7027	Medium		The ieee80211_radiotap_iterator_init function in net/wireless/radiotap.c in the Linux kernel before 3.11.7 does not check whether a frame contains any data outside of the header, which might allow attackers to cause a denial of service (buffer over-read) via a crafted header.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448732
7587	CVE-2013-7026	Medium		Multiple race conditions in ipc/shm.c in the Linux kernel before 3.12.2 allow local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via a crafted application that uses shmctl IPC_RMID operations in conjunction with other shm system calls.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448770
7588	CVE-2013-7024	Medium		The jpeg2000_decode_tile function in libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not consider the component number in certain calculations, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448735
7589	CVE-2013-7023	Medium		The ff_combine_frame function in libavcodec/parser.c in FFmpeg before 2.1 does not properly handle certain memory-allocation errors, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448728
7590	CVE-2013-7022	Medium		The g2m_init_buffers function in libavcodec/g2meet.c in FFmpeg before 2.1 does not properly allocate memory for tiles, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Go2Webinar data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448773
7591	CVE-2013-7021	Medium		The filter_frame function in libavfilter/vf_fps.c in FFmpeg before 2.1 does not properly ensure the availability of FIFO content, which allows remote attackers to cause a denial of service (double free) or possibly have unspecified other impact via crafted data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448769
7592	CVE-2013-7020	Medium		The read_header function in libavcodec/ffv1dec.c in FFmpeg before 2.1 does not properly enforce certain bit-count and colorspace constraints, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted FFV1 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448752

	A	B	C	D	E	F	G	H	I	J	K	L	M
7593	CVE-2013-7019	Medium		The get_cox function in libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not properly validate the reduction factor, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448760
7594	CVE-2013-7018	Medium		libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not ensure the use of valid code-block dimension values, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448767
7595	CVE-2013-7017	Medium		libavcodec/jpeg2000.c in FFmpeg before 2.1 allows remote attackers to cause a denial of service (invalid pointer dereference) or possibly have unspecified other impact via crafted JPEG2000 data.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448730
7596	CVE-2013-7016	Medium		The get_siz function in libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not ensure the expected sample separation, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448748
7597	CVE-2013-7015	Medium		The flashsv_decode_frame function in libavcodec/flashsv.c in FFmpeg before 2.1 does not properly validate a certain height value, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Flash Screen Video data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448764
7598	CVE-2013-7014	Medium		Integer signedness error in the add_bytes_l2_c function in libavcodec/pngdsp.c in FFmpeg before 2.1 allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted PNG data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448721
7599	CVE-2013-7013	Medium		The g2m_init_buffers function in libavcodec/g2meet.c in FFmpeg before 2.1 uses an incorrect ordering of arithmetic operations, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Go2Webinar data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448768
7600	CVE-2013-7012	Medium		The get_siz function in libavcodec/jpeg2000dec.c in FFmpeg before 2.1 does not prevent attempts to use non-zero image offsets, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG2000 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448724
7601	CVE-2013-7011	Medium		The read_header function in libavcodec/ffv1dec.c in FFmpeg before 2.1 does not prevent changes to global parameters, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted FFV1 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448740
7602	CVE-2013-7010	Medium		Multiple integer signedness errors in libavcodec/dsputil.c in FFmpeg before 2.1 allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448757
7603	CVE-2013-7009	Medium		The rpza_decode_stream function in libavcodec/rpza.c in FFmpeg before 2.1 does not properly maintain a pointer to pixel data, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted Apple RPZA data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448731
7604	CVE-2013-7008	Medium		The decode_slice_header function in libavcodec/h264.c in FFmpeg before 2.1 incorrectly relies on a certain droppable field, which allows remote attackers to cause a denial of service (deadlock) or possibly have unspecified other impact via crafted H.264 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448737
7605	CVE-2013-6954	Medium		The png_do_expand_palette function in libpng before 1.6.8 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via (1) a PLTE chunk of zero bytes or (2) a NULL palette, related to pngrtran.c and pngset.c.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6583
7606	CVE-2013-6891	Low		lppasswd in CUPS before 1.7.1, when running with setuid privileges, allows local users to read portions of arbitrary files via a modified HOME environment variable and a symlink attack involving .cups/client.conf.	cups	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6784
7607	CVE-2013-6858	Low		Multiple cross-site scripting (XSS) vulnerabilities in OpenStack Dashboard (Horizon) 2013.2 and earlier allow local users to inject arbitrary web script or HTML via an instance name to (1) Volumes or (2) Network Topology page.	openstack horizon.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445870
7608	CVE-2013-6800	Medium		An unspecified third-party database module for the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.10.x allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted request, a different vulnerability than CVE-2013-1418.CWE-476: NULL Pointer Dereference per http://cwe.mitre.org/data/definitions/476.html	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445829
7609	CVE-2013-6763	Medium		The uio_mmap_physical function in drivers/uio/uio.c in the Linux kernel before 3.12 does not validate the size of a memory block, which allows local users to cause a denial of service (memory corruption) or possibly gain privileges via crafted mmap operations, a different vulnerability than CVE-2013-4511.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444048
7610	CVE-2013-6501	Medium		The default soap.wsdl_cache_dir setting in (1) php.ini-production and (2) php.ini-development in PHP through 5.6.7 specifies the /tmp directory, which makes it easier for local users to conduct WSDL injection attacks by creating a file under /tmp with a predictable filename that is used by the get_sdl function in ext/soap/php_sdl.c.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-279

	A	B	C	D	E	F	G	H	I	J	K	L	M
7611	CVE-2013-6491	Medium		The python-qpid client (common/rpc/impl_qpid.py) in OpenStack Oslo before 2013.2 does not enforce SSL connections when qpid_protocol is set to ssl, which allows remote attackers to obtain sensitive information by sniffing the network.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1668
7612	CVE-2013-6476	Medium		The OPVPWrapper::loadDriver function in oprs/OPVPWrapper.cxx in the pdftoopvp filter in CUPS and cups-filters before 1.0.47 allows local users to gain privileges via a Trojan horse driver in the same directory as the PDF file.	cups	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7021
7613	CVE-2013-6475	Medium		Multiple integer overflows in (1) OPVPOutputDev.cxx and (2) oprs/OPVPSplash.cxx in the pdftoopvp filter in CUPS and cups-filters before 1.0.47 allow remote attackers to execute arbitrary code via a crafted PDF file, which triggers a heap-based buffer overflow.	cups	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7036
7614	CVE-2013-6474	Medium		Heap-based buffer overflow in the pdftoopvp filter in CUPS and cups-filters before 1.0.47 allows remote attackers to execute arbitrary code via a crafted PDF file.	cups	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7037
7615	CVE-2013-6470	Medium		The default configuration in the standalone controller quickstack manifest in openstack-foreman-installer, as used in Red Hat Enterprise Linux OpenStack Platform 4.0, disables authentication for Qpid, which allows remote attackers to gain access by connecting to Qpid.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1933
7616	CVE-2013-6468	Medium		JBoss Drools, Red Hat JBoss BRMS before 6.0.1, and Red Hat JBoss BPM Suite before 6.0.1 allows remote authenticated users to execute arbitrary Java code via a (1) MVFLEX Expression Language (MVEL) or (2) Drools expression.	jboss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1795
7617	CVE-2013-6466	Medium		Openswan 2.6.39 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and IKE daemon restart) via IKEv2 packets that lack expected payloads.	openswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6757
7618	CVE-2013-6462	High		Stack-based buffer overflow in the bdfReadCharacters function in bitmap/bdfread.c in X.Org libXfont 1.1 through 1.4.6 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string in a character name in a BDF font file.	libxfont	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6588
7619	CVE-2013-6458	Low		Multiple race conditions in the (1) virDomainBlockStats, (2) virDomainGetBlockInf, (3) qemuDomainBlockJobImpl, and (4) virDomainGetBlockIoTune functions in libvirt before 1.2.1 do not properly verify that the disk is attached, which allows remote read-only attackers to cause a denial of service (libvirtd crash) via the virDomainDetachDeviceFlags command.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6713
7620	CVE-2013-6457	Medium		The libxlDomainGetNumaParameters function in the libxl driver (libxl/libxl_driver.c) in libvirt before 1.2.1 does not properly initialize the nodemap, which allows local users to cause a denial of service (invalid free operation and crash) or possibly execute arbitrary code via an inactive domain to the virsh numatune command.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6739
7621	CVE-2013-6456	Medium		The LXC driver (lxc/lxc_driver.c) in libvirt 1.0.1 through 1.2.1 allows local users to (1) delete arbitrary host devices via the virDomainDeviceDettach API and a symlink attack on /dev in the container; (2) create arbitrary nodes (mknod) via the virDomainDeviceAttach API and a symlink attack on /dev in the container; and cause a denial of service (shutdown or reboot host OS) via the (3) virDomainShutdown or (4) virDomainReboot API and a symlink attack on /dev/initctl in the container, related to paths under /proc/$PID/root and the virInitctlSetRunLevel function.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7288
7622	CVE-2013-6450	Medium		The DTLS retransmission implementation in OpenSSL through 0.9.8y and 1.x through 1.0.1e does not properly maintain data structures for digest and encryption contexts, which might allow man-in-the-middle attackers to trigger the use of a different context by interfering with packet delivery, related to ssl/d1_both.c and ssl/t1_enc.c.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6580
7623	CVE-2013-6449	Medium		The ssl_get_algorithm2 function in ssl/s3_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect data structure, which allows remote attackers to cause a denial of service (daemon crash) via crafted traffic from a TLS 1.2 client.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6591
7624	CVE-2013-6442	Medium		The owner_set function in smbcacls.c in smbcacls in Samba 4.0.x before 4.0.16 and 4.1.x before 4.1.6 removes an ACL during use of a --chown or --chgrp option, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging an unintended administrative change.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7018
7625	CVE-2013-6441	High		The lxc-sshd template (templates/lxc-sshd.in) in LXC before 1.0.0.beta2 uses read-write permissions when mounting /sbin/init, which allows local users to gain privileges by modifying the init file.	lxc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6880
7626	CVE-2013-6438	Medium		The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7023
7627	CVE-2013-6437	Medium		The libvirt driver in OpenStack Compute (Nova) before 2013.2.2 and icehouse before icehouse-2 allows remote authenticated users to cause a denial of service (disk consumption) by creating and deleting instances with unique os_type settings, which triggers the creation of a new ephemeral disk backing file.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1730

	A	B	C	D	E	F	G	H	I	J	K	L	M
7628	CVE-2013-6436	Low		The lxcDomainGetMemoryParameters method in lxc/lxc_driver.c in libvirt 1.0.5 through 1.2.0 does not properly check the status of LXC guests when reading memory tunables, which allows local users to cause a denial of service (NULL pointer dereference and libvirtd crash) via a guest in the shutdown status, as demonstrated by the virsh memtune command.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6577
7629	CVE-2013-6435	High		Race condition in RPM 4.11.1 and earlier allows remote attackers to execute arbitrary code via a crafted RPM file whose installation extracts the contents to temporary files before validating the signature, as demonstrated by installing a file in the /etc/cron.d directory.	rpm	Unchanged	8.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2563
7630	CVE-2013-6433	High		The default configuration in the Red Hat openstack-neutron package before 2013.2.3-7 does not properly set a configuration file for rootwrap, which allows remote attackers to gain privileges via a crafted configuration file.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1928
7631	CVE-2013-6432	Medium		The ping_recvmsg function in net/ipv4/ping.c in the Linux kernel before 3.12.4 does not properly interact with read system calls on ping sockets, which allows local users to cause a denial of service (NULL pointer dereference and system crash) by leveraging unspecified privileges to execute a crafted application.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448729
7632	CVE-2013-6431	Medium		The fib6_add function in net/ipv6/ip6_fib.c in the Linux kernel before 3.11.5 does not properly implement error-code encoding, which allows local users to cause a denial of service (NULL pointer dereference and system crash) by leveraging the CAP_NET_ADMIN capability for an IPv6 SIOCADDRT ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448718
7633	CVE-2013-6428	Medium		The ReST API in OpenStack Orchestration API (Heat) before Havana 2013.2.1 and Icehouse before icehouse-2 allows remote authenticated users to bypass the tenant scoping restrictions via a modified tenant_id in the request path.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1658
7634	CVE-2013-6426	Medium		The cloudformation-compatible API in OpenStack Orchestration API (Heat) before Havana 2013.2.1 and Icehouse before icehouse-2 does not properly enforce policy rules, which allows local in-instance users to bypass intended access restrictions and (1) create a stack via the CreateStack method or (2) update a stack via the UpdateStack method.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1673
7635	CVE-2013-6425	Medium		Integer underflow in the pixman_trapezoid_valid macro in pixman.h in Pixman before 0.32.0, as used in X.Org server and cairo, allows context-dependent attackers to cause a denial of service (crash) via a negative bottom value.	pixman	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6728
7636	CVE-2013-6424	Medium		Integer underflow in the xTrapezoidValid macro in render/picture.h in X.Org allows context-dependent attackers to cause a denial of service (crash) via a negative bottom value.	x.org	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6751
7637	CVE-2013-6422	Medium		The GnuTLS backend in libcurl 7.21.4 through 7.33.0, when disabling digital signature verification (CURLOPT_SSL_VERIFYPEER), also disables the CURLOPT_SSL_VERIFYHOST check for CN or SAN host name fields, which makes it easier for remote attackers to spoof servers and conduct man-in-the-middle (MITM) attacks.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2509
7638	CVE-2013-6420	High		The asn1_time_to_time_t function in ext/openssl/openssl.c in PHP before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7 does not properly parse (1) notBefore and (2) notAfter timestamps in X.509 certificates, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate that is not properly handled by the openssl_x509_parse function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2516
7639	CVE-2013-6419	Medium		Interaction error in OpenStack Nova and Neutron before Havana 2013.2.1 and icehouse-1 does not validate the instance ID of the tenant making a request, which allows remote tenants to obtain sensitive metadata by spoofing the device ID that is bound to a port, which is not properly handled by (1) api/metadata/handler.py in Nova and (2) the neutron-metadata-agent (agent/metadata/agent.py) in Neutron.	openstack havana.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1575
7640	CVE-2013-6408	Medium		The DocumentAnalysisRequestHandler in Apache Solr before 4.3.1 does not properly use the EmptyEntityResolver, which allows remote attackers to have an unspecified impact via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-6407.	apache solr	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448754
7641	CVE-2013-6407	Medium		The UpdateRequestHandler for XML in Apache Solr before 4.1 allows remote attackers to have an unspecified impact via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.	apache solr	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448766
7642	CVE-2013-6400	Medium		Xen 4.2.x and 4.3.x, when using Intel VT-d and a PCI device has been assigned, does not clear the flag that suppresses IOMMU TLB flushes when unspecified errors occur, which causes the TLB entries to not be flushed and allows local guest administrators to cause a denial of service (host crash) or gain privileges via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1662
7643	CVE-2013-6399	High		Array index error in the virtio_load function in hw/virtio/virtio.c in QEMU before 1.7.2 allows remote attackers to execute arbitrary code via a crafted savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8760

	A	B	C	D	E	F	G	H	I	J	K	L	M
7644	CVE-2013-6398	Medium		The virtual router in Apache CloudStack before 4.2.1 does not preserve the source restrictions in firewall rules after being restarted, which allows remote attackers to bypass intended restrictions via a request.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6775
7645	CVE-2013-6397	Medium		Directory traversal vulnerability in SolrResourceLoader in Apache Solr before 4.6 allows remote attackers to read arbitrary files via a .. (dot dot) or full pathname in the tr parameter to solr/select/, when the response writer (wt parameter) is set to XSLT. NOTE: this can be leveraged using a separate XXE (XML eXternal Entity) vulnerability to allow access to files across restricted network boundaries.	apache solr	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448744
7646	CVE-2013-6396	Medium		The OpenStack Python client library for Swift (python-swiftclient) 1.0 through 1.9.0 does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	openstack swift	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1710
7647	CVE-2013-6393	Medium		The yaml_parser_scan_tag_uri function in scanner.c in LibYAML before 0.1.5 performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via crafted tags in a YAML document, which triggers a heap-based buffer overflow.	libyaml	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6734
7648	CVE-2013-6392	Medium		The genlock_dev_ioctl function in genlock.c in the Genlock driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not properly initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted GENLOCK_IOC_EXPORT ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6781
7649	CVE-2013-6391	Medium		The ec2tokens API in OpenStack Identity (Keystone) before Havana 2013.2.1 and Icehouse before icehouse-2 does not return a trust-scoped token when one is received, which allows remote trust users to gain privileges by generating EC2 credentials from a trust-scoped token and using them in an ec2tokens API request.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1666
7650	CVE-2013-6384	Low		(1) impl_db2.py and (2) impl_mongodb.py in OpenStack Ceilometer 2013.2 and earlier, when the logging level is set to INFO, logs the connection string from ceilometer.conf, which allows local users to obtain sensitive information (the DB2 or MongoDB password) by reading the log file.	openstack ceilometer.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445869
7651	CVE-2013-6383	Medium		The aac_compat_ioctl function in drivers/scsi/aacraid/linit.c in the Linux kernel before 3.11.8 does not require the CAP_SYS_RAWIO capability, which allows local users to bypass intended access restrictions via a crafted ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6764
7652	CVE-2013-6382	Medium		Multiple buffer underflows in the XFS implementation in the Linux kernel through 3.12.1 allow local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging the CAP_SYS_ADMIN capability for a (1) XFS_IOC_ATTRLIST_BY_HANDLE or (2) XFS_IOC_ATTRLIST_BY_HANDLE_32 ioctl call with a crafted length value, related to the xfs_attrlist_by_handle function in fs/xfs/xfs_ioctl.c and the xfs_compat_attrlist_by_handle function in fs/xfs/xfs_ioctl32.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6770
7653	CVE-2013-6381	Medium		Buffer overflow in the qeth_snmp_command function in drivers/s390/net/qeth_core_main.c in the Linux kernel through 3.12.1 allows local users to cause a denial of service or possibly have unspecified other impact via an SNMP ioctl call with a length value that is incompatible with the command-buffer size.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6747
7654	CVE-2013-6380	Medium		The aac_send_raw_srb function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 3.12.1 does not properly validate a certain size value, which allows local users to cause a denial of service (invalid pointer dereference) or possibly have unspecified other impact via an FSACTL_SEND_RAW_SRB ioctl call that triggers a crafted SRB command.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6754
7655	CVE-2013-6378	Medium		The lbs_debugfs_write function in drivers/net/wireless/libertas/debugfs.c in the Linux kernel through 3.12.1 allows local users to cause a denial of service (OOPS) by leveraging root privileges for a zero-length write operation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6722
7656	CVE-2013-6376	Medium		The recalculate_apic_map function in arch/x86/kvm/lapic.c in the KVM subsystem in the Linux kernel through 3.12.5 allows guest OS users to cause a denial of service (host OS crash) via a crafted ICR write operation in x2apic mode.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6731
7657	CVE-2013-6368	Medium		The KVM subsystem in the Linux kernel through 3.12.5 allows local users to gain privileges or cause a denial of service (system crash) via a VAPIC synchronization operation involving a page-end address.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6765
7658	CVE-2013-6367	Medium		The apic_get_tmcct function in arch/x86/kvm/lapic.c in the KVM subsystem in the Linux kernel through 3.12.5 allows guest OS users to cause a denial of service (divide-by-zero error and host OS crash) via crafted modifications of the TMICT value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6746
7659	CVE-2013-6357	Medium		** DISPUTED ** Cross-site request forgery (CSRF) vulnerability in the Manager application in Apache Tomcat 5.5.25 and earlier allows remote attackers to hijack the authentication of administrators for requests that manipulate application deployment via the POST method, as demonstrated by a /manager/html/undeploy?path= URI. NOTE: the vendor disputes the significance of this report, stating that the Apache Tomcat Security team has not accepted any reports of CSRF attacks against the Manager application ... as they require a reckless system administrator.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6723

	A	B	C	D	E	F	G	H	I	J	K	L	M
7660	CVE-2013-6282	High		The (1) get_user and (2) put_user API functions in the Linux kernel before 3.5.5 on the v6k and v7 ARM platforms do not validate certain addresses, which allows attackers to read or modify the contents of arbitrary kernel memory locations via a crafted application, as exploited in the wild against Android devices in October and November 2013.AV:L per https://www.codeaurora.org/projects/security-advisories/missing-access-checks-putusergetuser-kernel-api-cve-2013-6282	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445859
7661	CVE-2013-6230	Medium		The Winsock WSAIoctl API in Microsoft Windows Server 2008, as used in ISC BIND 9.6-ESV before 9.6-ESV-R10-P1, 9.8 before 9.8.6-P1, 9.9 before 9.9.4-P1, 9.9.3-S1, 9.9.4-S1, and other products, does not properly support the SIO_GET_INTERFACE_LIST command for netmask 255.255.255.255, which allows remote attackers to bypass intended IP address restrictions by leveraging misinterpretation of this netmask as a 0.0.0.0 netmask.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444032
7662	CVE-2013-6123	Medium		Multiple array index errors in drivers/media/video/msm/server/msm_cam_server.c in the MSM camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to gain privileges by leveraging camera device-node access, related to the (1) msm_ctrl_cmd_done, (2) msm_ioctl_server, and (3) msm_server_send_ctrl functions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6720
7663	CVE-2013-6122	Medium		goodix_tool.c in the Goodix gt915 touchscreen driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not properly synchronize updates to a global variable, which allows local users to bypass intended access restrictions or cause a denial of service (memory corruption) via crafted arguments to the procfs write handler.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444039
7664	CVE-2013-6076	Medium		strongSwan 5.0.2 through 5.1.0 allows remote attackers to cause a denial of service (NULL pointer dereference and charon daemon crash) via a crafted IKEv1 fragmentation packet.CWE-476: NULL Pointer Dereference per http://cwe.mitre.org/data/definitions/476.html	strongswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00442239
7665	CVE-2013-6075	Medium		The compare_dn function in utils/identification.c in strongSwan 4.3.3 through 5.1.1 allows (1) remote attackers to cause a denial of service (out-of-bounds read, NULL pointer dereference, and daemon crash) or (2) remote authenticated users to impersonate arbitrary users and bypass access restrictions via a crafted ID_DER_ASN1_DN ID, related to an insufficient length check during identity comparison.Per http://www.strongswan.org/blog/2013/11/01/strongswan-denial-of-service-vulnerability-%28cve-2013-6075%29.html 'Affected are strongSwan versions 4.3.3 and newer, up to 5.1.0.'	strongswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00442232
7666	CVE-2013-6051	Medium		The bgp_attr_unknown function in bgp_attr.c in Quagga 0.99.21 does not properly initialize the total variable, which allows remote attackers to cause a denial of service (bgpd crash) via a crafted BGP update.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6762
7667	CVE-2013-5908	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier allows remote attackers to affect availability via unknown vectors related to Error Handling.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6782
7668	CVE-2013-5894	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6730
7669	CVE-2013-5891	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.33 and earlier and 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6717
7670	CVE-2013-5882	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Stored Procedures.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6721
7671	CVE-2013-5881	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2014-0431.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6768
7672	CVE-2013-5860	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.14 and earlier allows remote authenticated users to affect availability via vectors related to GIS.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6786
7673	CVE-2013-5807	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.x through 5.5.32 and 5.6.x through 5.6.12 allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441886
7674	CVE-2013-5793	Low		Unspecified vulnerability in Oracle MySQL Server 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441876
7675	CVE-2013-5786	Medium		Unspecified vulnerability in Oracle MySQL Server 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441883
7676	CVE-2013-5770	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Locking.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441884
7677	CVE-2013-5767	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441890

	A	B	C	D	E	F	G	H	I	J	K	L	M
7678	CVE-2013-5724	Low		Phpbb3 before 3.0.11-4 for Debian GNU/Linux uses world-writable permissions for cache files, which allows local users to modify the file contents via standard filesystem write operations.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00434771
7679	CVE-2013-5704	Medium		The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass RequestHeader unset directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states this is not a security issue in httpd as such.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7268
7680	CVE-2013-5700	Medium		The Bloom Filter implementation in bitcoind and Bitcoin-Qt 0.8.x before 0.8.4rc1 allows remote attackers to cause a denial of service (divide-by-zero error and daemon crash) via a crafted sequence of messages.	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00434774
7681	CVE-2013-5653	Medium	Medium	The getenv and filenameforall functions in Ghostscript 9.10 ignore the -dSAFER argument, which allows remote attackers to read data via a crafted postscript file.	ghostscript	Unchanged	8.0.0.16	9.0.0.5	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3523
7682	CVE-2013-5651	Medium		The virBitmapParse function in util/virbitmap.c in libvirt before 1.1.2 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via a crafted bitmap, as demonstrated by a large nodeset value to numatune.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439173
7683	CVE-2013-5634	Medium		arch/arm/kvm/arm.c in the Linux kernel before 3.10 on the ARM platform, when KVM is used, allows host OS users to cause a denial of service (NULL pointer dereference, OOPS, and host OS crash) or possibly have unspecified other impact by omitting vCPU initialization before a KVM_GET_REG_LIST ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439165
7684	CVE-2013-5606	Medium		The CERT_VerifyCert function in lib/certhigh/certvfy.c in Mozilla Network Security Services (NSS) 3.15 before 3.15.3 provides an unexpected return value for an incompatible key-usage certificate when the CERTVerifyLog argument is valid, which might allow remote attackers to bypass intended access restrictions via a crafted certificate.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445831
7685	CVE-2013-5605	High		Mozilla Network Security Services (NSS) 3.14 before 3.14.5 and 3.15 before 3.15.3 allows remote attackers to cause a denial of service or possibly have unspecified other impact via invalid handshake packets.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445874
7686	CVE-2013-5228	Medium		WebKit, as used in Apple Safari before 6.1.1 and 7.x before 7.0.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-12-16-1.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2515
7687	CVE-2013-5225	Medium		WebKit, as used in Apple Safari before 6.1.1 and 7.x before 7.0.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-12-16-1.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2512
7688	CVE-2013-5211	Medium		The monlist feature in ntp_request.c in ntpd in NTP before 4.2.7p26 allows remote attackers to cause a denial of service (traffic amplification) via forged (1) REQ_MON_GETLIST or (2) REQ_MON_GETLIST_1 requests, as exploited in the wild in December 2013.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6582
7689	CVE-2013-5199	Medium		WebKit, as used in Apple Safari before 6.1.1 and 7.x before 7.0.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-12-16-1.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2519
7690	CVE-2013-5198	Medium		WebKit, as used in Apple Safari before 6.1.1 and 7.x before 7.0.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-12-16-1.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2523
7691	CVE-2013-5197	Medium		WebKit, as used in Apple Safari before 6.1.1 and 7.x before 7.0.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-12-16-1.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2508
7692	CVE-2013-5196	Medium		WebKit, as used in Apple Safari before 6.1.1 and 7.x before 7.0.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-12-16-1.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2513
7693	CVE-2013-5195	Medium		WebKit, as used in Apple Safari before 6.1.1 and 7.x before 7.0.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-12-16-1.	webkit	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2520
7694	CVE-2013-5036	High		The Square Squash allows remote attackers to execute arbitrary code via a YAML document in the (1) namespace parameter to the deobfuscation function or (2) sourcemap parameter to the sourcemap function in app/controllers/api/v1_controller.rb.	squash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7581
7695	CVE-2013-5029	Medium		phpMyAdmin 3.5.x and 4.0.x before 4.0.5 allows remote attackers to bypass the clickjacking protection mechanism via certain vectors related to Header.class.php.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433043

	A	B	C	D	E	F	G	H	I	J	K	L	M
7696	CVE-2013-5018	Medium		The is_asn1 function in strongSwan 4.1.11 through 5.0.4 does not properly validate the return value of the asn1_length function, which allows remote attackers to cause a denial of service (segmentation fault) via a (1) XAuth username, (2) EAP identity, or (3) PEM encoded file that starts with a 0x04, 0x30, or 0x31 character followed by an ASN.1 length value that triggers an integer overflow.	strongswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433019
7697	CVE-2013-5003	Medium		Multiple SQL injection vulnerabilities in phpMyAdmin 3.5.x before 3.5.8.2 and 4.0.x before 4.0.4.2 allow remote authenticated users to execute arbitrary SQL commands via (1) the scale parameter to pmd_pdf.php or (2) the pdf_page_number parameter to schema_export.php.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430972
7698	CVE-2013-5002	Low		Cross-site scripting (XSS) vulnerability in libraries/schema/Export_Relation_Schema.class.php in phpMyAdmin 3.5.x before 3.5.8.2 and 4.0.x before 4.0.4.2 allows remote authenticated users to inject arbitrary web script or HTML via a crafted pageNumber value to schema_export.php.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430962
7699	CVE-2013-5001	Low		Cross-site scripting (XSS) vulnerability in libraries/plugins/transformations/abstract/TextLinkTransformationsPlugin.class.php in phpMyAdmin 4.0.x before 4.0.4.2 allows remote authenticated users to inject arbitrary web script or HTML via a crafted object name associated with a TextLinkTransformationPlugin link.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430957
7700	CVE-2013-5000	Medium		phpMyAdmin 3.5.x before 3.5.8.2 allows remote attackers to obtain sensitive information via an invalid request, which reveals the installation path in an error message, related to config.default.php and other files.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430958
7701	CVE-2013-4999	Medium		phpMyAdmin 4.0.x before 4.0.4.2 allows remote attackers to obtain sensitive information via an invalid request, which reveals the installation path in an error message, related to Error.class.php and Error_Handler.class.php.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430965
7702	CVE-2013-4998	Medium		phpMyAdmin 3.5.x before 3.5.8.2 and 4.0.x before 4.0.4.2 allows remote attackers to obtain sensitive information via an invalid request, which reveals the installation path in an error message, related to pmd_common.php and other files.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430966
7703	CVE-2013-4997	Medium		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 3.5.x before 3.5.8.2 allow remote attackers to inject arbitrary web script or HTML via vectors involving a JavaScript event in (1) an anchor identifier to setup/index.php or (2) a chartTitle (aka chart title) value.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430963
7704	CVE-2013-4996	Medium		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 3.5.x before 3.5.8.2 and 4.0.x before 4.0.4.2 allow remote attackers to inject arbitrary web script or HTML via vectors involving (1) a crafted database name, (2) a crafted user name, (3) a crafted logo URL in the navigation panel, (4) a crafted entry in a certain proxy list, or (5) crafted content in a version.json file.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430956
7705	CVE-2013-4995	Low		Cross-site scripting (XSS) vulnerability in phpMyAdmin 3.5.x before 3.5.8.2 and 4.0.x before 4.0.4.2 allows remote authenticated users to inject arbitrary web script or HTML via a crafted SQL query that is not properly handled during the display of row information.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430971
7706	CVE-2013-4788	Medium		The PTR_MANGLE implementation in the GNU C Library (aka glibc or libc6) 2.4, 2.17 and earlier, and Embedded GLIBC (EGLIBC) does not initialize the random value for the pointer guard, which makes it easier for context-dependent attackers to control execution flow by leveraging a buffer-overflow vulnerability in an application and using the known zero value pointer guard to calculate a pointer address.Additional information that was taken into consideration while scoring: https://bugzilla.redhat.com/show_bug.cgi?id=985625	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439170
7707	CVE-2013-4758	Medium		Double free vulnerability in the writeDataError function in the ElasticSearch plugin (omelasticsearch) in rsyslog before 7.4.2 and before 7.5.2 devel, when errorfile is set to local logging, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted JSON response.	rsyslog	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439204
7708	CVE-2013-4740	Medium		goodix_tool.c in the Goodix gt915 touchscreen driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, relies on user-space length values for kernel-memory copies of procfs file content, which allows attackers to gain privileges or cause a denial of service (memory corruption) via an application that provides crafted values.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444029
7709	CVE-2013-4739	Medium		The MSM camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to obtain sensitive information from kernel stack memory via (1) a crafted MSM_MCR_IOCTL_EVT_GET ioctl call, related to drivers/media/platform/msm/camera_v1/mercury/msm_mercury_sync.c, or (2) a crafted MSM_JPEG_IOCTL_EVT_GET ioctl call, related to drivers/media/platform/msm/camera_v2/jpeg_10/msm_jpeg_sync.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6745

	A	B	C	D	E	F	G	H	I	J	K	L	M
7710	CVE-2013-4738	High		Multiple stack-based buffer overflows in the MSM camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to gain privileges via (1) a crafted VIDIOC_MSM_VPE_DEQUEUE_STREAM_BUFF_INFO ioctl call, related to drivers/media/platform/msm/camera_v2/proc/vpe/msm_vpe.c, or (2) a crafted VIDIOC_MSM_CPP_DEQUEUE_STREAM_BUFF_INFO ioctl call, related to drivers/media/platform/msm/camera_v2/proc/cpp/msm_cpp.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6755
7711	CVE-2013-4736	High		Multiple integer overflows in the JPEG engine drivers in the MSM camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service (system crash) via a large number of commands in an ioctl call, related to (1) camera_v1/gemini/msm_gemini_sync.c, (2) camera_v2/gemini/msm_gemini_sync.c, (3) camera_v2/jpeg_10/msm_jpeg_sync.c, (4) gemini/msm_gemini_sync.c, (5) jpeg_10/msm_jpeg_sync.c, and (6) mercury/msm_mercury_sync.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6761
7712	CVE-2013-4729	Medium		import.php in phpMyAdmin 4.x before 4.0.4.1 does not properly restrict the ability of input data to specify a file format, which allows remote authenticated users to modify the GLOBALS superglobal array, and consequently change the configuration, via a crafted request.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426604
7713	CVE-2013-4636	Medium		The mget function in libmagic/softmagic.c in the Fileinfo component in PHP 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (invalid pointer dereference and application crash) via an MP3 file that triggers incorrect MIME type detection during access to an finfo object.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424720
7714	CVE-2013-4635	Medium		Integer overflow in the SdnToJewish function in jewish.c in the Calendar component in PHP before 5.3.26 and 5.4.x before 5.4.16 allows context-dependent attackers to cause a denial of service (application hang) via a large argument to the jdtojewish function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424708
7715	CVE-2013-4592	Medium		Memory leak in the __kvm_set_memory_region function in virt/kvm/kvm_main.c in the Linux kernel before 3.9 allows local users to cause a denial of service (memory consumption) by leveraging certain device access to trigger movement of memory slots.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445863
7716	CVE-2013-4591	Medium		Buffer overflow in the __nfs4_get_acl_uncached function in fs/nfs/nfs4proc.c in the Linux kernel before 3.7.2 allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact via a getxattr system call for the system.nfs4_acl extended attribute of a pathname on an NFSv4 filesystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445844
7717	CVE-2013-4588	Medium		Multiple stack-based buffer overflows in net/netfilter/ipvs/ip_vs_ctl.c in the Linux kernel before 2.6.33, when CONFIG_IP_VS is used, allow local users to gain privileges by leveraging the CAP_NET_ADMIN capability for (1) a getsockopt system call, related to the do_ip_vs_get_ctl function, or (2) a setsockopt system call, related to the do_ip_vs_set_ctl function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445843
7718	CVE-2013-4587	High		Array index error in the kvm_vm_ioctl_create_vcpu function in virt/kvm/kvm_main.c in the KVM subsystem in the Linux kernel through 3.12.5 allows local users to gain privileges via a large id value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6733
7719	CVE-2013-4579	Medium		The ath9k_htc_set_bssid_mask function in drivers/net/wireless/ath/ath9k/htc_drv_main.c in the Linux kernel through 3.12 uses a BSSID masking approach to determine the set of MAC addresses on which a Wi-Fi device is listening, which allows remote attackers to discover the original MAC address after spoofing by sending a series of packets to MAC addresses with certain bit manipulations.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445832
7720	CVE-2013-4578			jarsigner in OpenJDK and Oracle Java SE before 7u51 allows remote attackers to bypass a code-signing protection mechanism and inject unsigned bytecode into a signed JAR file by leveraging improper file validation.	jdk & jre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-8525
7721	CVE-2013-4577	Low		A certain Debian patch for GNU GRUB uses world-readable permissions for grub.cfg, which allows local users to obtain password hashes, as demonstrated by reading the password_pbkdf2 directive in the file.	grub	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7430
7722	CVE-2013-4576	Low		GnuPG 1.x before 1.4.16 generates RSA keys using sequences of introductions with certain patterns that introduce a side channel, which allows physically-proximate attackers to extract RSA keys via a chosen-ciphertext attack and acoustic cryptanalysis during decryption. NOTE: applications are not typically expected to protect themselves from acoustic side-channel attacks, since this is arguably the responsibility of the physical device. Accordingly, issues of this type would not normally receive a CVE identifier. However, for this issue, the developer has specified a security policy in which GnuPG should offer side-channel resistance, and developer-specified security-policy violations are within the scope of CVE.	gnupg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2518
7723	CVE-2013-4563	High		The udp6_ufo_fragment function in net/ipv6/udp_offload.c in the Linux kernel through 3.12, when UDP Fragmentation Offload (UFO) is enabled, does not properly perform a certain size comparison before inserting a fragment header, which allows remote attackers to cause a denial of service (panic) via a large IPv6 UDP packet, as demonstrated by use of the Token Bucket Filter (TBF) queueing discipline.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445841

	A	B	C	D	E	F	G	H	I	J	K	L	M
7724	CVE-2013-4560	Low		Use-after-free vulnerability in lighttpd before 1.4.33 allows remote attackers to cause a denial of service (segmentation fault and crash) via unspecified vectors that trigger FAMMonitorDirectory failures.	lighttpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445834
7725	CVE-2013-4559	High		lighttpd before 1.4.33 does not check the return value of the (1) setuid, (2) setgid, or (3) setgroups functions, which might cause lighttpd to run as root if it is restarted and allows remote attackers to gain privileges, as demonstrated by multiple calls to the clone function that cause setuid to fail when the user process limit is reached.	lighttpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445864
7726	CVE-2013-4558	Low		The get_parent_resource function in repos.c in mod_dav_svn Apache HTTPD server module in Subversion 1.7.11 through 1.7.13 and 1.8.1 through 1.8.4, when built with assertions enabled and SVNAutoversioning is enabled, allows remote attackers to cause a denial of service (assertion failure and Apache process abort) via a non-canonical URL in a request, as demonstrated using a trailing /.	subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448736
7727	CVE-2013-4549	Medium		QXmlSimpleReader in Qt before 5.2 allows context-dependent attackers to cause a denial of service (memory consumption) via an XML Entity Expansion (XEE) attack.	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2507
7728	CVE-2013-4548	Medium		The mm_newkeys_from_blob function in monitor_wrap.c in sshd in OpenSSH 6.2 and 6.3, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444037
7729	CVE-2013-4545	Medium		cURL and libcurl 7.18.0 through 7.32.0, when built with OpenSSL, disables the certificate CN and SAN name field verification (CURLOPT_SSL_VERIFYHOST) when the digital signature verification (CURLOPT_SSL_VERIFYPEER) is disabled, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445853
7730	CVE-2013-4544	Medium		hw/net/vmxnet3.c in QEMU 2.0.0-rc0, 1.7.1, and earlier allows local guest users to cause a denial of service or possibly execute arbitrary code via vectors related to (1) RX or (2) TX queue numbers or (3) interrupt indices. NOTE: some of these details are obtained from third party information.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7415
7731	CVE-2013-4542	High		The virtio_scsi_load_request function in hw/scsi/scsi-bus.c in QEMU before 1.7.2 might allow remote attackers to execute arbitrary code via a crafted savevm image, which triggers an out-of-bounds array access.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8754
7732	CVE-2013-4541	High		The usb_device_post_load function in hw/usb/bus.c in QEMU before 1.7.2 might allow remote attackers to execute arbitrary code via a crafted savevm image, related to a negative setup_len or setup_index value.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8757
7733	CVE-2013-4540	High		Buffer overflow in scoop_gpio_handler_update in QEMU before 1.7.2 might allow remote attackers to execute arbitrary code via a large (1) prev_level, (2) gpio_level, or (3) gpio_dir value in a savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8746
7734	CVE-2013-4539	High		Multiple buffer overflows in the tsc210x_load function in hw/input/tsc210x.c in QEMU before 1.7.2 might allow remote attackers to execute arbitrary code via a crafted (1) precision, (2) nextprecision, (3) function, or (4) nextfunction value in a savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8758
7735	CVE-2013-4538	High		Multiple buffer overflows in the ssd0323_load function in hw/display/ssd0323.c in QEMU before 1.7.2 allow remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via crafted (1) cmd_len, (2) row, or (3) col values; (4) row_start and row_end values; or (5) col_star and col_end values in a savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8742
7736	CVE-2013-4537	High		The ssi_sd_transfer function in hw/sd/ssi-sd.c in QEMU before 1.7.2 allows remote attackers to execute arbitrary code via a crafted arglen value in a savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8751
7737	CVE-2013-4534	High		Buffer overflow in hw/intc/openpic.c in QEMU before 1.7.2 allows remote attackers to cause a denial of service or possibly execute arbitrary code via vectors related to IRQDest elements.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8741
7738	CVE-2013-4533	High		Buffer overflow in the pxa2xx_ssp_load function in hw/arm/pxa2xx.c in QEMU before 1.7.2 allows remote attackers to cause a denial of service or possibly execute arbitrary code via a crafted s->rx_level value in a savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8750
7739	CVE-2013-4531	High		Buffer overflow in target-arm/machine.c in QEMU before 1.7.2 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a negative value in cpreg_vmstate_array_len in a savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8753
7740	CVE-2013-4530	High		Buffer overflow in hw/ssi/pl022.c in QEMU before 1.7.2 allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted tx_fifo_head and rx_fifo_head values in a savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8747
7741	CVE-2013-4529	High		Buffer overflow in hw/pci/pcie_aer.c in QEMU before 1.7.2 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a large log_num value in a savevm image.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8745
7742	CVE-2013-4527	High		Buffer overflow in hw/timer/hpet.c in QEMU before 1.7.2 might allow remote attackers to execute arbitrary code via vectors related to the number of timers.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8739
7743	CVE-2013-4526	High		Buffer overflow in hw/ide/ahci.c in QEMU before 1.7.2 allows remote attackers to cause a denial of service and possibly execute arbitrary code via vectors related to migrating ports.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8749

	A	B	C	D	E	F	G	H	I	J	K	L	M
7744	CVE-2013-4520	Medium		xslt.c in libxslt before 1.1.25 allows context-dependent attackers to cause a denial of service (crash) via a stylesheet that embeds a DTD, which causes a structure to be accessed as a different type. NOTE: this issue is due to an incomplete fix for CVE-2012-2825.	libxslt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6598
7745	CVE-2013-4516	Medium		The mp_get_count function in drivers/staging/sb105x/sb_pci_mp.c in the Linux kernel before 3.12 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a TIOCGICOUNT ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444030
7746	CVE-2013-4515	Medium		The bcm_char_ioctl function in drivers/staging/bcm/Bcmchar.c in the Linux kernel before 3.12 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory via an IOCTL_BCM_GET_DEVICE_DRIVER_INFO ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444043
7747	CVE-2013-4514	Medium		Multiple buffer overflows in drivers/staging/wlags49_h2/wl_priv.c in the Linux kernel before 3.12 allow local users to cause a denial of service or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability and providing a long station-name string, related to the (1) wvlan_uil_put_info and (2) wvlan_set_station_nickname functions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444047
7748	CVE-2013-4513	Medium		Buffer overflow in the oz_cdev_write function in drivers/staging/ozwpan/ozcdev.c in the Linux kernel before 3.12 allows local users to cause a denial of service or possibly have unspecified other impact via a crafted write operation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444038
7749	CVE-2013-4512	Medium		Buffer overflow in the exitcode_proc_write function in arch/um/kernel/exitcode.c in the Linux kernel before 3.12 allows local users to cause a denial of service or possibly have unspecified other impact by leveraging root privileges for a write operation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444026
7750	CVE-2013-4511	Medium		Multiple integer overflows in Alchemy LCD frame-buffer drivers in the Linux kernel before 3.12 allow local users to create a read-write memory mapping for the entirety of kernel memory, and consequently gain privileges, via crafted mmap operations, related to the (1) au1100fb_fb_mmap function in drivers/video/au1100fb.c and the (2) au1200fb_fb_mmap function in drivers/video/au1200fb.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444052
7751	CVE-2013-4508	Medium		lighttpd before 1.4.34, when SNI is enabled, configures weak SSL ciphers, which makes it easier for remote attackers to hijack sessions by inserting packets into the client-server data stream or obtain sensitive information by sniffing the network.Per: http://download.lighttpd.net/lighttpd/security/lighttpd_sa_2013_01.txt All versions from 1.4.24 (first version supporting SNI) up to and including 1.4.33.	lighttpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444051
7752	CVE-2013-4505	Low		The is_this_legal function in mod_dontdothat for Apache Subversion 1.4.0 through 1.7.13 and 1.8.0 through 1.8.4 allows remote attackers to bypass intended access restrictions and possibly cause a denial of service (resource consumption) via a relative URL in a REPORT request.	apache subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448750
7753	CVE-2013-4497	Medium		The XenAPI backend in OpenStack Compute (Nova) Folsom, Grizzly, and Havana before 2013.2 does not properly apply security groups (1) when resizing an image or (2) during live migration, which allows remote attackers to bypass intended restrictions.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444053
7754	CVE-2013-4496	Medium		Samba 3.x before 3.6.23, 4.0.x before 4.0.16, and 4.1.x before 4.1.6 does not enforce the password-guessing protection mechanism for all interfaces, which makes it easier for remote attackers to obtain access via brute-force ChangePasswordUser2 (1) SAMR or (2) RAP attempts.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7032
7755	CVE-2013-4487	Medium		Off-by-one error in the dane_raw_tlsa in the DANE library (libdane) in GnuTLS 3.1.x before 3.1.16 and 3.2.x before 3.2.6 allows remote servers to cause a denial of service (memory corruption) via a response with more than four DANE entries. NOTE: this issue is due to an incomplete fix for CVE-2013-4466.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445873
7756	CVE-2013-4483	Medium		The ipc_rcu_putref function in ipc/util.c in the Linux kernel before 3.10 does not properly manage a reference count, which allows local users to cause a denial of service (memory consumption or system crash) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444033
7757	CVE-2013-4477	Low		The LDAP backend in OpenStack Identity (Keystone) Grizzly and Havana, when removing a role on a tenant for a user who does not have that role, adds the role to the user, which allows local users to gain privileges.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444046
7758	CVE-2013-4476	Low		Samba 4.0.x before 4.0.11 and 4.1.x before 4.1.1, when LDAP or HTTP is provided over SSL, uses world-readable permissions for a private key, which allows local users to obtain sensitive information by reading the key file, as demonstrated by access to the local filesystem on an AD domain controller.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444040
7759	CVE-2013-4475	Medium		Samba 3.x before 3.6.20, 4.0.x before 4.0.11, and 4.1.x before 4.1.1, when vfs_streams_depot or vfs_streams_xattr is enabled, allows remote attackers to bypass intended file restrictions by leveraging ACL differences between a file and an associated alternate data stream (ADS).	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444045
7760	CVE-2013-4474	Medium		Format string vulnerability in the extractPages function in utils/pdfseparate.cc in poppler before 024.2 allows remote attackers to cause a denial of service (crash) via format string specifiers in a destination filename.	poppler	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445849

	A	B	C	D	E	F	G	H	I	J	K	L	M
7761	CVE-2013-4473	High		Stack-based buffer overflow in the extractPages function in utils/pdfseparate.cc in poppler before 0.24.2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a source filename.	poppler	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445838
7762	CVE-2013-4471	Medium		The Identity v3 API in OpenStack Dashboard (Horizon) before 2013.2 does not require the current password when changing passwords for user accounts, which makes it easier for remote attackers to change a user password by leveraging the authentication token for that user.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1911
7763	CVE-2013-4470	High		The Linux kernel before 3.12, when UDP Fragmentation Offload (UFO) is enabled, does not properly initialize certain data structures, which allows local users to cause a denial of service (memory corruption and system crash) or possibly gain privileges via a crafted application that uses the UDP_CORK option in a setsockopt system call and sends both short and long packets, related to the ip_ufo_append_data function in net/ipv4/ip_output.c and the ip6_ufo_append_data function in net/ipv6/ip6_output.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444028
7764	CVE-2013-4469	Low		OpenStack Compute (Nova) Folsom, Grizzly, and Havana, when use_cow_images is set to False, does not verify the virtual size of a QCOW2 image, which allows local users to cause a denial of service (host file system disk consumption) by transferring an image with a large virtual size that does not contain a large amount of data from Glance. NOTE: this issue is due to an incomplete fix for CVE-2013-2096.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444027
7765	CVE-2013-4466	Medium		Buffer overflow in the dane_query_tlsa function in the DANE library (libdane) in GnuTLS 3.1.x before 3.1.15 and 3.2.x before 3.2.5 allows remote servers to cause a denial of service (memory corruption) via a response with more than four DANE entries.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445868
7766	CVE-2013-4463	Low		OpenStack Compute (Nova) Folsom, Grizzly, and Havana does not properly verify the virtual size of a QCOW2 image, which allows local users to cause a denial of service (host file system disk consumption) via a compressed QCOW2 image. NOTE: this issue is due to an incomplete fix for CVE-2013-2096.	nova	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1669
7767	CVE-2013-4458	Medium		Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in GNU C Library (aka glibc or libc6) 2.18 and earlier allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers a large number of AF_INET6 address results. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-1914.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448775
7768	CVE-2013-4457	Medium		The Cocaine gem 0.4.0 through 0.5.2 for Ruby allows context-dependent attackers to execute arbitrary commands via a crafted has object, related to recursive variable interpolation.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444044
7769	CVE-2013-4449	Medium		The rwm overlay in OpenLDAP 2.4.23, 2.4.36, and earlier does not properly count references, which allows remote attackers to cause a denial of service (slapd crash) by unbinding immediately after a search request, which triggers rwm_conn_destroy to free the session context while it is being used by rwm_op_search.	openldap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	CGP6-211
7770	CVE-2013-4434	Medium		Dropbear SSH Server before 2013.59 generates error messages for a failed logon attempt with different time delays depending on whether the user account exists, which allows remote attackers to discover valid usernames.	dropbear	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441874
7771	CVE-2013-4428	Low		OpenStack Image Registry and Delivery Service (Glance) Folsom, Grizzly before 2013.1.4, and Havana before 2013.2, when the image_download policy is configured, does not properly restrict access to cached images, which allows remote authenticated users to read otherwise restricted images via an image UUID.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441872
7772	CVE-2013-4421	Medium		The buf_decompress function in packet.c in Dropbear SSH Server before 2013.59 allows remote attackers to cause a denial of service (memory consumption) via a compressed packet that has a large size when it is decompressed.	dropbear	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441881
7773	CVE-2013-4408	High		Buffer overflow in the dcerpc_read_ncacn_packet_done function in librpc/rpc/dcerpc_util.c in winbindd in Samba 3.x before 3.6.22, 4.0.x before 4.0.13, and 4.1.x before 4.1.3 allows remote AD domain controllers to execute arbitrary code via an invalid fragment length in a DCE-RPC packet.	samba.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448727
7774	CVE-2013-4402	Medium		GnuPG 1.4.x before 1.4.15 and 2.0.x before 2.0.22 allows remote attackers to cause a denial of service (infinite recursion) via a crafted OpenPGP message.	gnupg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441877
7775	CVE-2013-4401	High		The virConnectDomainXMLToNative API function in libvirt 1.1.0 checks for the connect:read permission instead of the connect:write permission, which allows attackers to gain domain:write privileges and execute Qemu binaries via crafted XML. NOTE: some of these details are obtained from third party information.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444031
7776	CVE-2013-4400	High		virt-login-shell in libvirt 1.1.2 through 1.1.3 allows local users to overwrite arbitrary files and possibly gain privileges via unspecified environment variables or command-line arguments.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448765
7777	CVE-2013-4399	MEDIUM		The remoteClientFreeFunc function in daemon/remote.c in libvirt before 1.1.3, when ACLs are used, does not set an identity, which causes event handler removal to be denied and remote attackers to cause a denial of service (use-after-free and crash) by registering an event handler and then closing the connection.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2437

	A	B	C	D	E	F	G	H	I	J	K	L	M
7778	CVE-2013-4396	Medium		Use-after-free vulnerability in the doImageText function in dix/dixfonts.c in the xorg-server module before 1.14.4 in X.Org X11 allows remote authenticated users to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted ImageText request that triggers memory-allocation failure.Per: https://bugzilla.redhat.com/show_bug.cgi?id=1014561 ' A malicious, authorized client could use this flaw to crash the X.Org server or, potentially, execute arbitrary code with root privileges.'	xorg_x11.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439167
7779	CVE-2013-4387	Medium		net/ipv6/ip6_output.c in the Linux kernel through 3.11.4 does not properly determine the need for UDP Fragmentation Offload (UFO) processing of small packets after the UFO queueing of a large packet, which allows remote attackers to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact via network traffic that triggers a large response packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439176
7780	CVE-2013-4377	Low		Use-after-free vulnerability in the virtio-pci implementation in Qemu 1.4.0 through 1.6.0 allows local users to cause a denial of service (daemon crash) by hot-unplugging a virtio device.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441878
7781	CVE-2013-4375	Low		The qdisk PV disk backend in qemu-xen in Xen 4.2.x and 4.3.x before 4.3.1, and qemu 1.1 and other versions, allows local HVM guests to cause a denial of service (domain grant reference consumption) via unspecified vectors.	xen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1667
7782	CVE-2013-4363	Medium		Algorithmic complexity vulnerability in Gem::Version::ANCHORED_VERSION_PATTERN in lib/rubygems/version.rb in RubyGems before 1.8.23.2, 1.8.24 through 1.8.26, 2.0.x before 2.0.10, and 2.1.x before 2.1.5, as used in Ruby 1.9.0 through 2.0.0p247, allows remote attackers to cause a denial of service (CPU consumption) via a crafted gem version that triggers a large amount of backtracking in a regular expression. NOTE: this issue is due to an incomplete fix for CVE-2013-4287.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441880
7783	CVE-2013-4359	Medium		Integer overflow in kbdint.c in mod_sftp in ProFTPD 1.3.4d and 1.3.5r3 allows remote attackers to cause a denial of service (memory consumption) via a large response count value in an authentication request, which triggers a large memory allocation.	proftpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439183
7784	CVE-2013-4358	Medium		libavcodec/h264.c in FFmpeg before 0.11.4 allows remote attackers to cause a denial of service (crash) via vectors related to alternating bit depths in H.264 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2514
7785	CVE-2013-4354	Low		The API before 2.1 in OpenStack Image Registry and Delivery Service (Glance) makes it easier for local users to inject images into arbitrary tenants by adding the tenant as a member of the image.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445857
7786	CVE-2013-4353	Medium		The ssl3_take_mac function in ssl/s3_both.c in OpenSSL 1.0.1 before 1.0.1f allows remote TLS servers to cause a denial of service (NULL pointer dereference and application crash) via a crafted Next Protocol Negotiation record in a TLS handshake.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6575
7787	CVE-2013-4352	Medium		The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6, when a caching forward proxy is enabled, allows remote HTTP servers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger a missing hostname value.CWE-476: NULL Pointer Dereference	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8065
7788	CVE-2013-4351	Medium		GnuPG 1.4.x, 2.0.x, and 2.1.x treats a key flags subpacket with all bits cleared (no usage permitted) as if it has all bits set (all usage permitted), which might allow remote attackers to bypass intended cryptographic protection mechanisms by leveraging the subkey.	gnupg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439197
7789	CVE-2013-4350	Medium		The IPv6 SCTP implementation in net/sctp/ipv6.c in the Linux kernel through 3.11.1 uses data structures and function calls that do not trigger an intended configuration of IPsec encryption, which allows remote attackers to obtain sensitive information by sniffing the network.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439215
7790	CVE-2013-4348	High		The skb_flow_dissect function in net/core/flow_dissector.c in the Linux kernel through 3.12 allows remote attackers to cause a denial of service (infinite loop) via a small value in the IHL field of a packet with IPIP encapsulation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444042
7791	CVE-2013-4345	Medium		Off-by-one error in the get_prng_bytes function in crypto/ansi_cprng.c in the Linux kernel through 3.11.4 makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms via multiple requests for small amounts of data, leading to improper management of the state of the consumed data.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439207
7792	CVE-2013-4344	Medium		Buffer overflow in the SCSI implementation in QEMU, as used in Xen, when a SCSI controller has more than 256 attached devices, allows local users to gain privileges via a small transfer buffer in a REPORT LUNS command.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439187
7793	CVE-2013-4343	Medium		Use-after-free vulnerability in drivers/net/tun.c in the Linux kernel through 3.11.1 allows local users to gain privileges by leveraging the CAP_NET_ADMIN capability and providing an invalid tuntap interface name in a TUNSETIFF ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439175
7794	CVE-2013-4342	High		xinetd does not enforce the user and group configuration directives for TCPMUX services, which causes these services to be run as root and makes it easier for remote attackers to gain privileges by leveraging another vulnerability in a service.	xinetd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439216

	A	B	C	D	E	F	G	H	I	J	K	L	M
7795	CVE-2013-4332	Medium		Multiple integer overflows in malloc/malloc.c in the GNU C Library (aka glibc or libc6) 2.18 and earlier allow context-dependent attackers to cause a denial of service (heap corruption) via a large value to the (1) pvalloc, (2) valloc, (3) posix_memalign, (4) memalign, or (5) aligned_alloc functions.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439192
7796	CVE-2013-4330	Medium		Apache Camel before 2.9.7, 2.10.0 before 2.10.7, 2.11.0 before 2.11.2, and 2.12.0 allows remote attackers to execute arbitrary simple language expressions by including $simple{} in a CamelFileName message header to a (1) FILE or (2) FTP producer.	apache camel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439166
7797	CVE-2013-4316	High		Apache Struts 2.0.0 through 2.3.15.1 enables Dynamic Method Invocation by default, which has unknown impact and attack vectors.	apache struts	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439177
7798	CVE-2013-4312	MEDIUM		The Linux kernel before 4.4.1 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by sending each descriptor over a UNIX socket before closing it, related to net/unix/af_unix.c and net/unix/garbage.c.	linux	Unchanged	8.0.0.3	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-246
7799	CVE-2013-4311	Medium		libvirt 1.0.5.x before 1.0.5.6, 0.10.2.x before 0.10.2.8, and 0.9.12.x before 0.9.12.2 allows local users to bypass intended access restrictions by leveraging a PolkitUnixProcess PolkitSubject race condition in pkcheck via a (1) setuid process or (2) pkexec process, a related issue to CVE-2013-4288.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439206
7800	CVE-2013-4310	Medium		Apache Struts 2.0.0 through 2.3.15.1 allows remote attackers to bypass access controls via a crafted action: prefix.	apache struts	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439191
7801	CVE-2013-4300	High		The scm_check_creds function in net/core/scm.c in the Linux kernel before 3.11 performs a capability check in an incorrect namespace, which allows local users to gain privileges via PID spoofing.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439178
7802	CVE-2013-4299	Medium		Interpretation conflict in drivers/md/dm-snap-persistent.c in the Linux kernel through 3.11.6 allows remote authenticated users to obtain sensitive information or modify data via a crafted mapping to a snapshot block device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441888
7803	CVE-2013-4298	Medium		The ReadGIFImage function in coders/gif.c in ImageMagick before 6.7.8-8 allows remote attackers to cause a denial of service (memory corruption and application crash) via a crafted comment in a GIF image.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00434773
7804	CVE-2013-4297	Medium		The virFileNBDDeviceAssociate function in util/virfile.c in libvirt 1.1.2 and earlier allows remote authenticated users to cause a denial of service (uninitialized pointer dereference and crash) via unspecified vectors.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439189
7805	CVE-2013-4296	Medium		The remoteDispatchDomainMemoryStats function in daemon/remote.c in libvirt 0.9.1 through 0.10.1.x, 0.10.2.x before 0.10.2.8, 1.0.x before 1.0.5.6, and 1.1.x before 1.1.2 allows remote authenticated users to cause a denial of service (uninitialized pointer dereference and crash) via a crafted RPC call.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439171
7806	CVE-2013-4292	Low		libvirt 1.1.0 and 1.1.1 allows local users to cause a denial of service (memory consumption) via a large number of domain migrate parameters in certain RPC calls in (1) daemon/remote.c and (2) remote/remote_driver.c.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439210
7807	CVE-2013-4291	Medium		The virSecurityManagerSetProcessLabel function in libvirt 0.10.2.7, 1.0.5.5, and 1.1.1, when the domain has read an uid:gid label, does not properly set group memberships, which allows local users to gain privileges.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439198
7808	CVE-2013-4287	Medium		Algorithmic complexity vulnerability in Gem::Version::VERSION_PATTERN in lib/rubygems/version.rb in RubyGems before 1.8.23.1, 1.8.24 through 1.8.25, 2.0.x before 2.0.8, and 2.1.x before 2.1.0, as used in Ruby 1.9.0 through 2.0.0p247, allows remote attackers to cause a denial of service (CPU consumption) via a crafted gem version that triggers a large amount of backtracking in a regular expression.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441870
7809	CVE-2013-4282	Medium		Stack-based buffer overflow in the reds_handle_ticket function in server/reds.c in SPICE 0.12.0 allows remote attackers to cause a denial of service (crash) via a long password in a SPICE ticket.	spice	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444049
7810	CVE-2013-4277	Low		Svnserve in Apache Subversion 1.4.0 through 1.7.12 and 1.8.0 through 1.8.1 allows local users to overwrite arbitrary files or kill arbitrary processes via a symlink attack on the file specified by the --pid-file option.	apache subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439199
7811	CVE-2013-4270	Low		The net_ctl_permissions function in net/sysctl_net.c in the Linux kernel before 3.11.5 does not properly determine uid and gid values, which allows local users to bypass intended /proc/sys/net restrictions via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448758
7812	CVE-2013-4265	High		The av_reallocp_array function in libavutil/mem.c in FFmpeg before 2.0.1 has an unspecified impact and remote vectors related to a wrong return code and a resultant NULL pointer dereference.http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445830
7813	CVE-2013-4264	Medium		The kempf_decode_tile function in libavcodec/g2meet.c in FFmpeg before 2.0.1 allows remote attackers to cause a denial of service (out-of-bounds heap write) via a G2M4 encoded file.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445851
7814	CVE-2013-4263	High		libavfilter in FFmpeg before 2.0.1 allows has unspecified impact and remote vectors related to a crafted plane, which triggers an out-of-bounds heap write.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445858
7815	CVE-2013-4262	Low		svnwcsub.py in Subversion 1.8.0 before 1.8.3, when using the --pidfile option and running in foreground mode, allows local users to gain privileges via a symlink attack on the pid file. NOTE: this issue was SPLIT due to different affected versions (ADT3). The irkerbridge.py issue is covered by CVE-2013-7393.	subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8071

	A	B	C	D	E	F	G	H	I	J	K	L	M
7816	CVE-2013-4261	Low		OpenStack Compute (Nova) Folsom, Grizzly, and earlier, when using Apache Qpid for the RPC backend, does not properly handle errors that occur during messaging, which allows remote attackers to cause a denial of service (connection pool consumption), as demonstrated using multiple requests that send long strings to an instance console and retrieving the console log.	openstack compute	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441887
7817	CVE-2013-4254	Medium		The validate_event function in arch/arm/kernel/perf_event.c in the Linux kernel before 3.10.8 on the ARM platform allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) by adding a hardware event to an event group led by a software event.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433040
7818	CVE-2013-4248	Medium		The openssl_x509_parse function in openssl.c in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433025
7819	CVE-2013-4247	High		Off-by-one error in the build_unc_path_to_root function in fs/cifs/connect.c in the Linux kernel before 3.9.6 allows remote attackers to cause a denial of service (memory corruption and system crash) via a DFS share mount operation that triggers use of an unexpected DFS referral name length.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433032
7820	CVE-2013-4246			libsvn_fs_fs/fs_fs.c in Apache Subversion 1.8.x before 1.8.2 might allow remote authenticated users with commit access to corrupt FSFS repositories and cause a denial of service or obtain sensitive information by editing packed revision properties.	subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-2504
7821	CVE-2013-4244	Medium		The LZW decompressor in the gif2tiff tool in libtiff 4.0.3 and earlier allows context-dependent attackers to cause a denial of service (out-of-bounds write and crash) or possibly execute arbitrary code via a crafted GIF image.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439163
7822	CVE-2013-4243	Medium		Heap-based buffer overflow in the readgifimage function in the gif2tiff tool in libtiff 4.0.3 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted height and width values in a GIF image.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00434772
7823	CVE-2013-4242	Low		GnuPG before 1.4.14, and Libgcrypt before 1.5.3 as used in GnuPG 2.0.x and possibly other products, allows local users to obtain private RSA keys via a cache side-channel attack involving the L3 cache, aka Flush+Reload.	gnupg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433037
7824	CVE-2013-4239	Medium		The xenDaemonListDefinedDomains function in xen/xend_internal.c in libvirt 1.1.1 allows remote authenticated users to cause a denial of service (memory corruption and crash) via vectors involving the virConnectListDefinedDomains API function.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439184
7825	CVE-2013-4238	Medium		The ssl.match_hostname function in the SSL module in Python 2.6 through 3.4 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433035
7826	CVE-2013-4237	Medium		sysdeps/posix/readdir_r.c in the GNU C Library (aka glibc or libc6) 2.18 and earlier allows context-dependent attackers to cause a denial of service (out-of-bounds write and crash) or possibly execute arbitrary code via a crafted (1) NTFS or (2) CIFS image.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439209
7827	CVE-2013-4236	Low		VDSM in Red Hat Enterprise Virtualization 3 and 3.2 allows privileged guest users to cause the host to become unavailable to the managment server via invalid XML characters in a guest agent response. NOTE: this issue is due to an incomplete fix for CVE-2013-0167.	vdsm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444036
7828	CVE-2013-4232	Medium		Use-after-free vulnerability in the t2p_readwrite_pdf_image function in tools/tiff2pdf.c in libtiff 4.0.3 allows remote attackers to cause a denial of service (crash) or possible execute arbitrary code via a crafted TIFF image.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00434770
7829	CVE-2013-4231	Medium		Multiple buffer overflows in libtiff before 4.0.3 allow remote attackers to cause a denial of service (out-of-bounds write) via a crafted (1) extension block in a GIF image or (2) GIF raster image to tools/gif2tiff.c or (3) a long filename for a TIFF image to tools/rgb2ycbcr.c. NOTE: vectors 1 and 3 are disputed by Red Hat, which states that the input cannot exceed the allocated buffer size.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6758
7830	CVE-2013-4220	Medium		The bad_mode function in arch/arm64/kernel/traps.c in the Linux kernel before 3.9.5 on the ARM64 platform allows local users to cause a denial of service (system crash) via vectors involving an attempted register access that triggers an unexpected value in the Exception Syndrome Register (ESR).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433042
7831	CVE-2013-4214	Medium		rss-newsfeed.php in Nagios Core 3.4.4, 3.5.1, and earlier, when MAGPIE_CACHE_ON is set to 1, allows local users to overwrite arbitrary files via a symlink attack on /tmp/magpie_cache.per http://rhn.redhat.com/errata/RHSA-2013-1526.html 'Affected Products: Red Hat OpenStack 3.0'	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445866
7832	CVE-2013-4212	Medium		Certain getText methods in the ActionSupport controller in Apache Roller before 5.0.2 allow remote attackers to execute arbitrary OGNL expressions via the first or second parameter, as demonstrated by the pageTitle parameter in the !getPageTitle sub-URL to roller-ui/login.rol, which uses a subclass of UIAction, aka OGNL Injection.	apache solr	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448772

	A	B	C	D	E	F	G	H	I	J	K	L	M
7833	CVE-2013-4205	Medium		Memory leak in the unshare_userns function in kernel/user_namespace.c in the Linux kernel before 3.10.6 allows local users to cause a denial of service (memory consumption) via an invalid CLONE_NEWUSER unshare call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433029
7834	CVE-2013-4185	Medium		Algorithmic complexity vulnerability in OpenStack Compute (Nova) before 2013.1.3 and Havana before havana-3 does not properly handle network source security group policy updates, which allows remote authenticated users to cause a denial of service (nova-network consumption) via a large number of server-creation operations, which triggers a large number of update requests.	openstack compute	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441871
7835	CVE-2013-4181	Medium		Cross-site scripting (XSS) vulnerability in the addAlert function in the RedirectServlet servlet in oVirt Engine and Red Hat Enterprise Virtualization Manager (RHEV-M), as used in Red Hat Enterprise Virtualization 3 and 3.2, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	ovirt-engine	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444050
7836	CVE-2013-4171	Medium		Multiple cross-site scripting (XSS) vulnerabilities in Apache Roller before 5.0.2 allow remote attackers to inject arbitrary web script or HTML via vectors related to the search results in the (1) RSS and (2) Atom feed templates.	apache roller	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448751
7837	CVE-2013-4169	Medium		GNOME Display Manager (gdm) before 2.21.1 allows local users to change permissions of arbitrary directories via a symlink attack on /tmp/.X11-unix/.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00434769
7838	CVE-2013-4164	Medium		Heap-based buffer overflow in Ruby 1.8, 1.9 before 1.9.3-p484, 2.0 before 2.0.0-p353, 2.1 before 2.1.0 preview2, and trunk before revision 43780 allows context-dependent attackers to cause a denial of service (segmentation fault) and possibly execute arbitrary code via a string that is converted to a floating point value, as demonstrated using (1) the to_f method or (2) JSON.parse.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445879
7839	CVE-2013-4163	Medium		The ip6_append_data_mtu function in net/ipv6/ip6_output.c in the IPv6 implementation in the Linux kernel through 3.10.3 does not properly maintain information about whether the IPV6_MTU setsockopt option had been specified, which allows local users to cause a denial of service (BUG and system crash) via a crafted application that uses the UDP_CORK option in a setsockopt system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428872
7840	CVE-2013-4162	Medium		The udp_v6_push_pending_frames function in net/ipv6/udp.c in the IPv6 implementation in the Linux kernel through 3.10.3 makes an incorrect function call for pending data, which allows local users to cause a denial of service (BUG and system crash) via a crafted application that uses the UDP_CORK option in a setsockopt system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428885
7841	CVE-2013-4160	Medium		Little CMS (lcms2) before 2.5, as used in OpenJDK 7 and possibly other products, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to (1) cmsStageAllocLabV2ToV4curves, (2) cmsPipelineDup, (3) cmsAllocProfileSequenceDescription, (4) CurvesAlloc, and (5) cmsnamed.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	openjdk	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1659
7842	CVE-2013-4154	Medium		The qemuAgentCommand function in libvirt before 1.1.1, when a guest agent is not configured, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to agent based cpu (un)plug, as demonstrated by the virsh vcpucount foobar --guest command.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439196
7843	CVE-2013-4153	Medium		Double free vulnerability in the qemuAgentGetVCPUs function in qemu/qemu_agent.c in libvirt 1.0.6 through 1.1.0 allows remote attackers to cause a denial of service (daemon crash) via a cpu count request, as demonstrated by the virsh vcpucount dom --guest command.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439208
7844	CVE-2013-4151	High		The virtio_load function in virtio/virtio.c in QEMU 1.x before 1.7.2 allows remote attackers to execute arbitrary code via a crafted savevm image, which triggers an out-of-bounds write.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8759
7845	CVE-2013-4150	High		The virtio_net_load function in hw/net/virtio-net.c in QEMU 1.5.0 through 1.7.x before 1.7.2 allows remote attackers to cause a denial of service or possibly execute arbitrary code via vectors in which the value of curr_queues is greater than max_queues, which triggers an out-of-bounds write.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8740
7846	CVE-2013-4149	High		Buffer overflow in virtio_net_load function in net/virtio-net.c in QEMU 1.3.0 through 1.7.x before 1.7.2 might allow remote attackers to execute arbitrary code via a large MAC table.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8744
7847	CVE-2013-4148	High		Integer signedness error in the virtio_net_load function in hw/net/virtio-net.c in QEMU 1.x before 1.7.2 allows remote attackers to execute arbitrary code via a crafted savevm image, which triggers a buffer overflow.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8761
7848	CVE-2013-4131	Medium		The mod_dav_svn Apache HTTPD server module in Subversion 1.7.0 through 1.7.10 and 1.8.x before 1.8.1 allows remote authenticated users to cause a denial of service (assertion failure or out-of-bounds read) via a certain (1) COPY, (2) DELETE, or (3) MOVE request against a revision root.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430960
7849	CVE-2013-4129	Medium		The bridge multicast implementation in the Linux kernel through 3.10.3 does not check whether a certain timer is armed before modifying the timeout value of that timer, which allows local users to cause a denial of service (BUG and system crash) via vectors involving the shutdown of a KVM virtual machine, related to net/bridge/br_mdb.c and net/bridge/br_multicast.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428893

	A	B	C	D	E	F	G	H	I	J	K	L	M
7850	CVE-2013-4127	Medium		Use-after-free vulnerability in the vhost_net_set_backend function in drivers/vhost/net.c in the Linux kernel through 3.10.3 allows local users to cause a denial of service (OOPS and system crash) via vectors involving powering on a virtual machine.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428880
7851	CVE-2013-4125	Medium		The fib6_add_rt2node function in net/ipv6/ip6_fib.c in the IPv6 stack in the Linux kernel through 3.10.1 does not properly handle Router Advertisement (RA) messages in certain circumstances involving three routes that initially qualified for membership in an ECMP route set until a change occurred for one of the first two routes, which allows remote attackers to cause a denial of service (system crash) via a crafted sequence of messages.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428889
7852	CVE-2013-4124	Medium		Integer overflow in the read_nttrans_ea_list function in nttrans.c in smbd in Samba 3.x before 3.5.22, 3.6.x before 3.6.17, and 4.x before 4.0.8 allows remote attackers to cause a denial of service (memory consumption) via a malformed packet.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430959
7853	CVE-2013-4113	Medium		ext/xml/xml.c in PHP before 5.3.27 does not properly consider parsing depth, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted document that is processed by the xml_parse_into_struct function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428869
7854	CVE-2013-4111	Medium		The Python client library for Glance (python-glanceclient) before 0.10.0 does not properly check the preverify_ok value, which prevents the server hostname from being verified with a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate and allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433030
7855	CVE-2013-4073	Medium		The OpenSSL::SSL.verify_certificate_identity function in lib/openssl/ssl.rb in Ruby 1.8 before 1.8.7-p374, 1.9 before 1.9.3-p448, and 2.0 before 2.0.0-p247 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433034
7856	CVE-2013-4037	Medium		The RAKP protocol support in the Intelligent Platform Management Interface (IPMI) implementation in Integrated Management Module (IMM) and Integrated Management Module II (IMM2) on IBM BladeCenter, Flex System, System x iDataPlex, and System x3### servers sends a password hash to the client, which makes it easier for remote attackers to obtain access via a brute-force attack.	m4	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430973
7857	CVE-2013-3919	High		resolver.c in ISC BIND 9.8.5 before 9.8.5-P1, 9.9.3 before 9.9.3-P1, and 9.6-ESV-R9 before 9.6-ESV-R9-P1, when a recursive resolver is configured, allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for a record in a malformed zone.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421932
7858	CVE-2013-3839	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.70 and earlier, 5.5.32 and earlier, and 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441879
7859	CVE-2013-3812	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428866
7860	CVE-2013-3811	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3806.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428879
7861	CVE-2013-3810	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to XA Transactions.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428895
7862	CVE-2013-3809	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Audit Log.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428876
7863	CVE-2013-3808	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 allows remote authenticated users to affect availability via unknown vectors related to Server Options.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428897
7864	CVE-2013-3807	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect confidentiality and integrity via unknown vectors related to Server Privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428887
7865	CVE-2013-3806	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3811.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428881
7866	CVE-2013-3805	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.30 and earlier and 5.6.10 allows remote authenticated users to affect availability via unknown vectors related to Prepared Statements.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428870
7867	CVE-2013-3804	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428871

	A	B	C	D	E	F	G	H	I	J	K	L	M
7868	CVE-2013-3802	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.69 and earlier, 5.5.31 and earlier, and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Full Text Search.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428894
7869	CVE-2013-3801	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.30 and earlier and 5.6.10 allows remote authenticated users to affect availability via unknown vectors related to Server Options.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428882
7870	CVE-2013-3798	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect integrity and availability via unknown vectors related to MemCached.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428878
7871	CVE-2013-3796	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428886
7872	CVE-2013-3795	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428865
7873	CVE-2013-3794	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.30 and earlier and 5.6.10 allows remote authenticated users to affect availability via unknown vectors related to Server Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428896
7874	CVE-2013-3793	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428888
7875	CVE-2013-3783	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Parser.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428898
7876	CVE-2013-3742	Low		Cross-site scripting (XSS) vulnerability in view_create.php (aka the Create View page) in phpMyAdmin 4.x before 4.0.3 allows remote authenticated users to inject arbitrary web script or HTML via an invalid SQL CREATE VIEW statement with a crafted name that triggers an error message.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426615
7877	CVE-2013-3735	Medium		** DISPUTED ** The Zend Engine in PHP before 5.4.16 RC1, and 5.5.0 before RC2, does not properly determine whether a parser error occurred, which allows context-dependent attackers to cause a denial of service (memory consumption and application crash) via a crafted function definition, as demonstrated by an attack within a shared web-hosting environment. NOTE: the vendor's http://php.net/security-note.php page says for critical security situations you should be using OS-level security by running multiple web servers each as their own user id.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421922
7878	CVE-2013-3704	Medium		The RPM GPG key import and handling feature in libzypp 12.15.0 and earlier reports a different key fingerprint than the one used to sign a repository when multiple key blobs are used, which might allow remote attackers to trick users into believing that the repository was signed by a more-trustworthy key.	libzypp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441875
7879	CVE-2013-3675	Medium		The process_frame_obj function in sanm.c in libavcodec in FFmpeg before 1.2.1 does not validate width and height values, which allows remote attackers to cause a denial of service (integer overflow, out-of-bounds array access, and application crash) via crafted LucasArts Smush video data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421929
7880	CVE-2013-3674	Medium		The cdg_decode_frame function in cdgraphics.c in libavcodec in FFmpeg before 1.2.1 does not validate the presence of non-header data in a buffer, which allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) via crafted CD Graphics Video data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421903
7881	CVE-2013-3673	Medium		The gif_decode_frame function in gifdec.c in libavcodec in FFmpeg before 1.2.1 does not properly manage the disposal methods of frames, which allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) via crafted GIF data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421916
7882	CVE-2013-3672	Medium		The mm_decode_inter function in mmvideo.c in libavcodec in FFmpeg before 1.2.1 does not validate the relationship between a horizontal coordinate and a width value, which allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) via crafted American Laser Games (ALG) MM Video data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421923
7883	CVE-2013-3671	Medium		The format_line function in log.c in libavutil in FFmpeg before 1.2.1 uses inapplicable offset data during a certain category calculation, which allows remote attackers to cause a denial of service (invalid pointer dereference and application crash) via crafted data that triggers a log message.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421908
7884	CVE-2013-3670	Medium		The rle_unpack function in vmdav.c in libavcodec in FFmpeg git 20130328 through 20130501 does not properly use the bytestream2 API, which allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) via crafted RLE data. NOTE: the vendor has listed this as an issue fixed in 1.2.1, but the issue is actually in new code that was not shipped with the 1.2.1 release or any earlier release.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421917
7885	CVE-2013-3571	Low		socat 1.2.0.0 before 1.7.2.2 and 2.0.0-b1 before 2.0.0-b6, when used for a listen type address and the fork option is enabled, allows remote attackers to cause a denial of service (file descriptor consumption) via multiple request that are refused based on the (1) sourceport, (2) lowport, (3) range, or (4) tcpwrap restrictions.	socat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7431

	A	B	C	D	E	F	G	H	I	J	K	L	M
7886	CVE-2013-3302	Medium		Race condition in the smb_send_rqst function in fs/cifs/transport.c in the Linux kernel before 3.7.2 allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via vectors involving a reconnection event.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415929
7887	CVE-2013-3301	High		The ftrace implementation in the Linux kernel before 3.8.8 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by leveraging the CAP_SYS_ADMIN capability for write access to the (1) set_ftrace_pid or (2) set_graph_function file, and then making an lseek system call.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415950
7888	CVE-2013-3271	Medium		EMC RSA Authentication Agent for PAM 7.0 before 7.0.2.1 enforces the maximum number of login attempts within the PAM-enabled application codebase, instead of within the Agent codebase, which makes it easier for remote attackers to discover correct login credentials via a brute-force attack.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433022
7889	CVE-2013-3241	Medium		export.php (aka the export script) in phpMyAdmin 4.x before 4.0.0-rc3 overwrites global variables on the basis of the contents of the POST superglobal array, which allows remote authenticated users to inject values via a crafted request.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415946
7890	CVE-2013-3240	Medium		Directory traversal vulnerability in the Export feature in phpMyAdmin 4.x before 4.0.0-rc3 allows remote authenticated users to read arbitrary files or possibly have unspecified other impact via a parameter that specifies a crafted export type.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415957
7891	CVE-2013-3239	Medium		phpMyAdmin 3.5.x before 3.5.8 and 4.x before 4.0.0-rc3, when a SaveDir directory is configured, allows remote authenticated users to execute arbitrary code by using a double extension in the filename of an export file, leading to interpretation of this file as an executable file by the Apache HTTP Server, as demonstrated by a .php.sql filename.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415964
7892	CVE-2013-3238	Medium		phpMyAdmin 3.5.x before 3.5.8 and 4.x before 4.0.0-rc3 allows remote authenticated users to execute arbitrary code via a /e\x00 sequence, which is not properly handled before making a preg_replace function call within the Replace table prefix feature.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415945
7893	CVE-2013-3237	Medium		The vsock_stream_sendmsg function in net/vmw_vsock/af_vsock.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415925
7894	CVE-2013-3236	Medium		The vmci_transport_dgram_dequeue function in net/vmw_vsock/vmci_transport.c in the Linux kernel before 3.9-rc7 does not properly initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415922
7895	CVE-2013-3235	Medium		net/tipc/socket.c in the Linux kernel before 3.9-rc7 does not initialize a certain data structure and a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415974
7896	CVE-2013-3234	Medium		The rose_recvmsg function in net/rose/af_rose.c in the Linux kernel before 3.9-rc7 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415953
7897	CVE-2013-3233	Medium		The llcp_sock_recvmsg function in net/nfc/llcp/sock.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable and a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415917
7898	CVE-2013-3232	Medium		The nr_recvmsg function in net/netrom/af_netrom.c in the Linux kernel before 3.9-rc7 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415963
7899	CVE-2013-3231	Medium		The llc_ui_recvmsg function in net/llc/af_llc.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415947
7900	CVE-2013-3230	Medium		The l2tp_ip6_recvmsg function in net/l2tp/l2tp_ip6.c in the Linux kernel before 3.9-rc7 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415930
7901	CVE-2013-3229	Medium		The iucv_sock_recvmsg function in net/iucv/af_iucv.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415914
7902	CVE-2013-3228	Medium		The irda_recvmsg_dgram function in net/irda/af_irda.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415965
7903	CVE-2013-3227	Medium		The caif_seqpkt_recvmsg function in net/caif/caif_socket.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415941

	A	B	C	D	E	F	G	H	I	J	K	L	M
7904	CVE-2013-3226	Medium		The sco_sock_recvmsg function in net/bluetooth/sco.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415927
7905	CVE-2013-3225	Medium		The rfcomm_sock_recvmsg function in net/bluetooth/rfcomm/sock.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415911
7906	CVE-2013-3224	Medium		The bt_sock_recvmsg function in net/bluetooth/af_bluetooth.c in the Linux kernel before 3.9-rc7 does not properly initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415958
7907	CVE-2013-3223	Medium		The ax25_recvmsg function in net/ax25/af_ax25.c in the Linux kernel before 3.9-rc7 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415937
7908	CVE-2013-3222	Medium		The vcc_recvmsg function in net/atm/common.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415918
7909	CVE-2013-3221	Medium		The Active Record component in Ruby on Rails 2.3.x, 3.0.x, 3.1.x, and 3.2.x does not ensure that the declared data type of a database column is used during comparisons of input values to stored values in that column, which makes it easier for remote attackers to conduct data-type injection attacks against Ruby on Rails applications via a crafted value, as demonstrated by unintended interaction between the typed XML feature and a MySQL database.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415971
7910	CVE-2013-3076	Medium		The crypto API in the Linux kernel through 3.9-rc8 does not initialize certain length variables, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call, related to the hash_recvmsg function in crypto/algif_hash.c and the skcipher_recvmsg function in crypto/algif_skcipher.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415915
7911	CVE-2013-3060	Medium		The web console in Apache ActiveMQ before 5.8.0 does not require authentication, which allows remote attackers to obtain sensitive information or cause a denial of service via HTTP requests.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415949
7912	CVE-2013-2944	Medium		strongSwan 4.3.5 through 5.0.3, when using the OpenSSL plugin for ECDSA signature verification, allows remote attackers to authenticate as other users via an invalid signature.	strongswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417547
7913	CVE-2013-2930	Low		The perf_trace_event_perm function in kernel/trace/trace_event_perf.c in the Linux kernel before 3.12.2 does not properly restrict access to the perf subsystem, which allows local users to enable function tracing via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448762
7914	CVE-2013-2929	Low		The Linux kernel before 3.12.2 does not properly use the get_dumpable function, which allows local users to bypass intended ptrace restrictions or obtain sensitive information from IA64 scratch registers via a crafted application, related to kernel/ptrace.c and arch/ia64/include/asm/processor.h.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448742
7915	CVE-2013-2924	High		Use-after-free vulnerability in International Components for Unicode (ICU), as used in Google Chrome before 30.0.1599.66 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.	icu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00443080
7916	CVE-2013-2899	Medium		drivers/hid/hid-picolcd_core.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_PICOLCD is enabled, allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) via a crafted device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439213
7917	CVE-2013-2898	Low		drivers/hid/hid-sensor-hub.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_SENSOR_HUB is enabled, allows physically proximate attackers to obtain sensitive information from kernel memory via a crafted device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439194
7918	CVE-2013-2897	Medium		Multiple array index errors in drivers/hid/hid-multitouch.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_MULTITOUCH is enabled, allow physically proximate attackers to cause a denial of service (heap memory corruption, or NULL pointer dereference and OOPS) via a crafted device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439185
7919	CVE-2013-2896	Medium		drivers/hid/hid-ntrig.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_NTRIG is enabled, allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) via a crafted device.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439169
7920	CVE-2013-2895	Medium		drivers/hid/hid-logitech-dj.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_LOGITECH_DJ is enabled, allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) or obtain sensitive information from kernel memory via a crafted device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439203

	A	B	C	D	E	F	G	H	I	J	K	L	M
7921	CVE-2013-2894	Medium		drivers/hid/hid-lenovo-tpkbd.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_LENOVO_TPKBD is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439188
7922	CVE-2013-2893	Medium		The Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_LOGITECH_FF, CONFIG_LOGIG940_FF, or CONFIG_LOGIWHEELS_FF is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device, related to (1) drivers/hid/hid-lgff.c, (2) drivers/hid/hid-lg3ff.c, and (3) drivers/hid/hid-lg4ff.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439180
7923	CVE-2013-2892	Medium		drivers/hid/hid-pl.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_PANTHERLORD is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439164
7924	CVE-2013-2891	Medium		drivers/hid/hid-steelseries.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_STEELSERIES is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439168
7925	CVE-2013-2890	Medium		drivers/hid/hid-sony.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_SONY is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439212
7926	CVE-2013-2889	Medium		drivers/hid/hid-zpff.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_ZEROPLUS is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439172
7927	CVE-2013-2888	Medium		Multiple array index errors in drivers/hid/hid-core.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11 allow physically proximate attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted device that provides an invalid Report ID.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439182
7928	CVE-2013-2877	Medium		parser.c in libxml2 before 2.9.0, as used in Google Chrome before 28.0.1500.71 and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a document that ends abruptly, related to the lack of certain checks for the XML_PARSER_EOF state.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426610
7929	CVE-2013-2852	Medium		Format string vulnerability in the b43_request_firmware function in drivers/net/wireless/b43/main.c in the Broadcom B43 wireless driver in the Linux kernel through 3.9.4 allows local users to gain privileges by leveraging root access and including format string specifiers in an fwpostfix modprobe parameter, leading to improper construction of an error message.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421911
7930	CVE-2013-2851	Medium		Format string vulnerability in the register_disk function in block/genhd.c in the Linux kernel through 3.9.4 allows local users to gain privileges by leveraging root access and writing format string specifiers to /sys/module/md_mod/parameters/new_array in order to create a crafted /dev/md device name.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421933
7931	CVE-2013-2850	High		Heap-based buffer overflow in the iscsi_add_notunderstood_response function in drivers/target/iscsi/iscsi_target_parameters.c in the iSCSI target subsystem in the Linux kernel through 3.9.4 allows remote attackers to cause a denial of service (memory corruption and OOPS) or possibly execute arbitrary code via a long key that is not properly handled during construction of an error-response packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421910
7932	CVE-2013-2777	Medium		sudo before 1.7.10p5 and 1.8.x before 1.8.6p6, when the tty_tickets option is enabled, does not properly validate the controlling terminal device, which allows local users with sudo permissions to hijack the authorization of another terminal via vectors related to a session without a controlling terminal device and connecting to a standard input, output, and error file descriptors of another terminal. NOTE: this is one of three closely-related vulnerabilities that were originally assigned CVE-2013-1776, but they have been SPLIT because of different affected versions.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413561
7933	CVE-2013-2776	Medium		sudo 1.3.5 through 1.7.10p5 and 1.8.0 through 1.8.6p6, when running on systems without /proc or the sysctl function with the tty_tickets option enabled, does not properly validate the controlling terminal device, which allows local users with sudo permissions to hijack the authorization of another terminal via vectors related to connecting to a standard input, output, and error file descriptors of another terminal. NOTE: this is one of three closely-related vulnerabilities that were originally assigned CVE-2013-1776, but they have been SPLIT because of different affected versions.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413547
7934	CVE-2013-2765	Medium		The ModSecurity module before 2.7.4 for the Apache HTTP Server allows remote attackers to cause a denial of service (NULL pointer dereference, process crash, and disk consumption) via a POST request with a large body and a crafted Content-Type header.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428875
7935	CVE-2013-2636	Low		net/bridge/br_mdb.c in the Linux kernel before 3.8.4 does not initialize certain structures, which allows local users to obtain sensitive information from kernel memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411220

	A	B	C	D	E	F	G	H	I	J	K	L	M
7936	CVE-2013-2635	Low		The rtnl_fill_ifinfo function in net/core/rtnetlink.c in the Linux kernel before 3.8.4 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411214
7937	CVE-2013-2634	Low		net/dcb/dcbnl.c in the Linux kernel before 3.8.4 does not initialize certain structures, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411204
7938	CVE-2013-2617	High		lib/curl.rb in the Curl Gem for Ruby allows remote attackers to execute arbitrary commands via shell metacharacters in a URL.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411200
7939	CVE-2013-2548	Low		The crypto_report_one function in crypto/crypto_user.c in the report API in the crypto user configuration API in the Linux kernel through 3.8.2 uses an incorrect length value during a copy operation, which allows local users to obtain sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413567
7940	CVE-2013-2547	Low		The crypto_report_one function in crypto/crypto_user.c in the report API in the crypto user configuration API in the Linux kernel through 3.8.2 does not initialize certain structure members, which allows local users to obtain sensitive information from kernel heap memory by leveraging the CAP_NET_ADMIN capability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413570
7941	CVE-2013-2546	Low		The report API in the crypto user configuration API in the Linux kernel through 3.8.2 uses an incorrect C library function for copying strings, which allows local users to obtain sensitive information from kernel stack memory by leveraging the CAP_NET_ADMIN capability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413584
7942	CVE-2013-2494	Medium		libdns in ISC DHCP 4.2.x before 4.2.5-P1 allows remote name servers to cause a denial of service (memory consumption) via vectors involving a regular expression, as demonstrated by a memory-exhaustion attack against a machine running a dhcpd process, a related issue to CVE-2013-2266.	dhcp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413349
7943	CVE-2013-2395	Medium		Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language, a different vulnerability than CVE-2013-1567.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415909
7944	CVE-2013-2392	Medium		Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415952
7945	CVE-2013-2391	Low		Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows local users to affect confidentiality and integrity via unknown vectors related to Server Install.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415959
7946	CVE-2013-2389	Medium		Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415919
7947	CVE-2013-2381	Low		Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server Privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415968
7948	CVE-2013-2378	Medium		Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier, 5.5.29 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Information Schema.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415923
7949	CVE-2013-2376	Medium		Unspecified vulnerability in Oracle MySQL 5.5.30 and earlier and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Stored Procedure.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415938
7950	CVE-2013-2375	Medium		Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415951
7951	CVE-2013-2266	High		libdns in ISC BIND 9.7.x and 9.8.x before 9.8.4-P2, 9.8.5 before 9.8.5b2, 9.9.x before 9.9.2-P2, and 9.9.3 before 9.9.3b2 on UNIX platforms allows remote attackers to cause a denial of service (memory consumption) via a crafted regular expression, as demonstrated by a memory-exhaustion attack against a machine running a named process.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413349
7952	CVE-2013-2251	High		Apache Struts 2.0.0 through 2.3.15 allows remote attackers to execute arbitrary OGNL expressions via a parameter with a crafted (1) action:, (2) redirect:, or (3) redirectAction: prefix.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428891
7953	CVE-2013-2250	High		Apache Open For Business Project (aka OFBiz) 10.04.01 through 10.04.05, 11.04.01 through 11.04.02, and 12.04.01 allows remote attackers to execute arbitrary Unified Expression Language (UEL) functions via JUEL metacharacters in unspecified parameters, related to nested expressions.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433026
7954	CVE-2013-2249	High		mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428874
7955	CVE-2013-2248	Medium		Multiple open redirect vulnerabilities in Apache Struts 2.0.0 through 2.3.15 allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in a parameter using the (1) redirect: or (2) redirectAction: prefix.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428877

	A	B	C	D	E	F	G	H	I	J	K	L	M
7956	CVE-2013-2239	Medium		vzkernel before 042stab080.2 in the OpenVZ modification for the Linux kernel 2.6.32 does not initialize certain length variables, which allows local users to obtain sensitive information from kernel stack memory via (1) a crafted ploop driver ioctl call, related to the ploop_getdevice_ioc function in drivers/block/ploop/dev.c or (2) a crafted quotactl system call, related to the compat_quotactl function in fs/quota/quota.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444034
7957	CVE-2013-2237	Low		The key_notify_policy_flush function in net/key/af_key.c in the Linux kernel before 3.9 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel heap memory by reading a broadcast message from the notify_policy interface of an IPSec key_socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426606
7958	CVE-2013-2236	Low		Stack-based buffer overflow in the new_msg_lsa_change_notify function in the OSPFD API (ospf_api.c) in Quagga before 0.99.22.2, when --enable-opaque-lsa and the -a command line option are used, allows remote attackers to cause a denial of service (crash) via a large LSA.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441885
7959	CVE-2013-2234	Low		The (1) key_notify_sa_flush and (2) key_notify_policy_flush functions in net/key/af_key.c in the Linux kernel before 3.10 do not initialize certain structure members, which allows local users to obtain sensitive information from kernel heap memory by reading a broadcast message from the notify interface of an IPSec key_socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426602
7960	CVE-2013-2232	Medium		The ip6_sk_dst_check function in net/ipv6/ip6_output.c in the Linux kernel before 3.10 allows local users to cause a denial of service (system crash) by using an AF_INET6 socket for a connection to an IPv4 interface.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426599
7961	CVE-2013-2230	Medium		The qemu driver (qemu/qemu_driver.c) in libvirt before 1.1.1 allows remote authenticated users to cause a denial of service (daemon crash) via unspecified vectors involving multiple events registration.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439201
7962	CVE-2013-2218	Medium		Double free vulnerability in the virConnectListAllInterfaces method in interface/interface_backend_netcf.c in libvirt 1.0.6 allows remote attackers to cause a denial of service (libvirtd crash) via a filtering flag that causes an interface to be skipped, as demonstrated by the virsh iface-list --inactive command.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439195
7963	CVE-2013-2210	High		Heap-based buffer overflow in the XML Signature Reference functionality in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.2 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via malformed XPointer expressions. NOTE: this is due to an incorrect fix for CVE-2013-2154.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433027
7964	CVE-2013-2207	Low		pt_chown in GNU C Library (aka glibc or libc6) before 2.18 does not properly check permissions for tty files, which allows local users to change the permission on the files and obtain access to arbitrary pseudo-terminals by leveraging a FUSE file system.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439202
7965	CVE-2013-2206	Medium		The sctp_sf_do_5_2_4_dupcook function in net/sctp/sm_statefuns.c in the SCTP implementation in the Linux kernel before 3.8.5 does not properly handle associations during the processing of a duplicate COOKIE ECHO chunk, which allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via crafted SCTP traffic.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426598
7966	CVE-2013-2185	High		** DISPUTED ** The readObject method in the DiskFileItem class in Apache Tomcat and JBoss Web, as used in Red Hat JBoss Enterprise Application Platform 6.1.0 and Red Hat JBoss Portal 6.0.0, allows remote attackers to write to arbitrary files via a NULL byte in a file name in a serialized instance, a similar issue to CVE-2013-2186. NOTE: this issue is reportedly disputed by the Apache Tomcat team, although Red Hat considers it a vulnerability. The dispute appears to regard whether it is the responsibility of applications to avoid providing untrusted data to be deserialized, or whether this class should inherently protect against this issue.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6741
7967	CVE-2013-2179	Medium		X.Org xdm 1.1.10, 1.1.11, and possibly other versions, when performing authentication using certain implementations of the crypt API function that can return NULL, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) by attempting to log into an account whose password field contains invalid characters, as demonstrated using the crypt function from glibc 2.17 and later with (1) the ! character in the salt portion of a password field or (2) a password that has been encrypted using DES or MD5 in FIPS-140 mode.	x.org	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2510
7968	CVE-2013-2174	Medium		Heap-based buffer overflow in the curl_easy_unescape function in lib/escape.c in cURL and libcurl 7.7 through 7.30.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string ending in a % (percent) character.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430970
7969	CVE-2013-2172	Medium		jcp/xml/dsig/internal/dom/DOMCanonicalizationMethod.java in Apache Santuario XML Security for Java 1.4.x before 1.4.8 and 1.5.x before 1.5.5 allows context-dependent attackers to spoof an XML Signature by using the CanonicalizationMethod parameter to specify an arbitrary weak canonicalization algorithm to apply to the SignedInfo part of the Signature.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433021
7970	CVE-2013-2168	Low		The _dbus_printf_string_upper_bound function in dbus/dbus-sysdeps-unix.c in D-Bus (aka DBus) 1.4.x before 1.4.26, 1.6.x before 1.6.12, and 1.7.x before 1.7.4 allows local users to cause a denial of service (service crash) via a crafted message.	dbus	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426607

	A	B	C	D	E	F	G	H	I	J	K	L	M
7971	CVE-2013-2164	Low		The mmc_ioctl_cdrom_read_data function in drivers/cdrom/cdrom.c in the Linux kernel through 3.10 allows local users to obtain sensitive information from kernel memory via a read operation on a malfunctioning CD-ROM drive.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426609
7972	CVE-2013-2160	Medium		Apache CXF 2.5.x before 2.5.10, 2.6.x before 2.6.7, and 2.7.x before 2.7.4 allows remote attackers to cause a denial of service (CPU and memory consumption) via crafted XML with a large number of (1) elements, (2) attributes, (3) nested constructs, and possibly other vectors.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433033
7973	CVE-2013-2156	High		Heap-based buffer overflow in the Exclusive Canonicalization functionality (xsec/canon/XSECC14n20010315.cpp) in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PrefixList attribute.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433020
7974	CVE-2013-2155	Medium		Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 does not properly validate length values, which allows remote attackers to cause a denial of service or bypass the CVE-2009-0217 protection mechanism and spoof a signature via crafted length values to the (1) compareBase64StringToRaw, (2) DSIGAlgorithmHandlerDefault, or (3) DSIGAlgorithmHandlerDefault::verify functions.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433039
7975	CVE-2013-2154	High		Stack-based buffer overflow in the XML Signature Reference functionality (xsec/dsig/DSIGReference.cpp) in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via malformed XPointer expressions, probably related to the DSIGReference::getURIBaseTXFM function.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433036
7976	CVE-2013-2153	Medium		The XML digital signature functionality (xsec/dsig/DSIGReference.cpp) in Apache Santuario XML Security for C++ (aka xml-security-c) before 1.7.1 allows context-dependent attackers to reuse signatures and spoof arbitrary content via crafted Reference elements in the Signature, aka XML Signature Bypass issue.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433028
7977	CVE-2013-2148	Low		The fill_event_metadata function in fs/notify/fanotify/fanotify_user.c in the Linux kernel through 3.9.4 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel memory via a read operation on the fanotify descriptor.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421919
7978	CVE-2013-2147	Low		The HP Smart Array controller disk-array driver and Compaq SMART2 controller disk-array driver in the Linux kernel through 3.9.4 do not initialize certain data structures, which allows local users to obtain sensitive information from kernel memory via (1) a crafted IDAGETPCIINFO command for a /dev/ida device, related to the ida_locked_ioctl function in drivers/block/cpqarray.c or (2) a crafted CCISS_PASSTHRU32 command for a /dev/cciss device, related to the cciss_ioctl32_passthru function in drivers/block/cciss.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421904
7979	CVE-2013-2146	Medium		arch/x86/kernel/cpu/perf_event_intel.c in the Linux kernel before 3.8.9, when the Performance Events Subsystem is enabled, specifies an incorrect bitmask, which allows local users to cause a denial of service (general protection fault and system crash) by attempting to set a reserved bit.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421905
7980	CVE-2013-2141	Low		The do_tkill function in kernel/signal.c in the Linux kernel before 3.8.9 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory via a crafted application that makes a (1) tkill or (2) tgkill system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421934
7981	CVE-2013-2140	Low		The dispatch_discard_io function in drivers/block/xen-blkback/blkback.c in the Xen blkback implementation in the Linux kernel before 3.10.5 allows guest OS users to cause a denial of service (data loss) via filesystem write operations on a read-only disk that supports the (1) BLKIF_OP_DISCARD (aka discard or TRIM) or (2) SCSI UNMAP feature.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439190
7982	CVE-2013-2137	Medium		Cross-site scripting (XSS) vulnerability in the View Log screen in the Webtools application in Apache Open For Business Project (aka OFBiz) 10.04.01 through 10.04.05, 11.04.01 through 11.04.02, and 12.04.01 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433018
7983	CVE-2013-2136	Medium		Multiple cross-site scripting (XSS) vulnerabilities in Apache CloudStack before 4.1.1 allow remote attackers to inject arbitrary web script or HTML via the (1) Physical network name to the Zone wizard; (2) New network name, (3) instance name, or (4) group to the Instance wizard; (5) unspecified multi-edit fields; and (6) unspecified list view edit fields related to global settings.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433041
7984	CVE-2013-2135	High		Apache Struts 2 before 2.3.14.3 allows remote attackers to execute arbitrary OGNL code via a request with a crafted value that contains both ${} and %{} sequences, which causes the OGNL code to be evaluated twice.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428892
7985	CVE-2013-2134	High		Apache Struts 2 before 2.3.14.3 allows remote attackers to execute arbitrary OGNL code via a request with a crafted action name that is not properly handled during wildcard matching, a different vulnerability than CVE-2013-2135.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428884
7986	CVE-2013-2130	Medium		ZNC 1.0 allows remote authenticated users to cause a denial of service (NULL pointer reference and crash) via a crafted request to the (1) editnetwork, (2) editchan, (3) addchan, or (4) delchan page in modules/webadmin.cpp.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference	znc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7667

	A	B	C	D	E	F	G	H	I	J	K	L	M
7987	CVE-2013-2128	Medium		The tcp_read_sock function in net/ipv4/tcp.c in the Linux kernel before 2.6.34 does not properly manage skb consumption, which allows local users to cause a denial of service (system crash) via a crafted splice system call for a TCP socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421924
7988	CVE-2013-2116	Medium		The _gnutls_ciphertext2compressed function in lib/gnutls_cipher.c in GnuTLS 2.12.23 allows remote attackers to cause a denial of service (buffer over-read and crash) via a crafted padding length. NOTE: this might be due to an incorrect fix for CVE-2013-0169.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426603
7989	CVE-2013-2115	High		Apache Struts 2 before 2.3.14.2 allows remote attackers to execute arbitrary OGNL code via a crafted request that is not properly handled when using the includeParams attribute in the (1) URL or (2) A tag. NOTE: this issue is due to an incomplete fix for CVE-2013-1966.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426613
7990	CVE-2013-2112	High		The svnserve server in Subversion before 1.6.23 and 1.7.x before 1.7.10 allows remote attackers to cause a denial of service (exit) by aborting a connection.	Subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430964
7991	CVE-2013-2110	Medium		Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424710
7992	CVE-2013-2099	Medium		Algorithmic complexity vulnerability in the ssl.match_hostname function in Python 3.2.x, 3.3.x, and earlier, and unspecified versions of python-backports-ssl_match_hostname as used for older Python versions, allows remote attackers to cause a denial of service (CPU consumption) via multiple wildcard characters in the common name in a certificate.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439186
7993	CVE-2013-2094	High		The perf_swevent_init function in kernel/events/core.c in the Linux kernel before 3.8.9 uses an incorrect integer data type, which allows local users to gain privileges via a crafted perf_event_open system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00419903
7994	CVE-2013-2088	High		contrib/hook-scripts/svn-keyword-check.pl in Subversion before 1.6.23 allows remote authenticated users with commit permissions to execute arbitrary commands via shell metacharacters in a filename.	Subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430968
7995	CVE-2013-2071	Low		java/org/apache/catalina/core/AsyncContextImpl.java in Apache Tomcat 7.x before 7.0.40 does not properly handle the throwing of a RuntimeException in an AsyncListener in an application, which allows context-dependent attackers to obtain sensitive request information intended for other applications in opportunistic circumstances via an application that records the requests that it processes.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421912
7996	CVE-2013-2067	Medium		java/org/apache/catalina/authenticator/FormAuthenticator.java in the form authentication feature in Apache Tomcat 6.0.21 through 6.0.36 and 7.x before 7.0.33 does not properly handle the relationships between authentication requirements and sessions, which allows remote attackers to inject a request into a session by sending this request during completion of the login form, a variant of a session fixation attack.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421907
7997	CVE-2013-2066	Medium		Buffer overflow in X.org libXv 1.0.7 and earlier allows X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the XvQueryPortAttributes function.	libxv	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424718
7998	CVE-2013-2065	Medium		(1) DL and (2) Fiddle in Ruby 1.9 before 1.9.3 patchlevel 426, and 2.0 before 2.0.0 patchlevel 195, do not perform taint checking for native functions, which allows context-dependent attackers to bypass intended $SAFE level restrictions.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444041
7999	CVE-2013-2064	Medium		Integer overflow in X.org libxcb 1.9 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the read_packet function.	libxcb	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424729
8000	CVE-2013-2063	Medium		Integer overflow in X.org libXtst 1.2.1 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the XRecordGetContext function.	libxtst	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424702
8001	CVE-2013-2062	Medium		Multiple integer overflows in X.org libXp 1.0.1 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XpGetAttributes, (2) XpGetOneAttribute, (3) XpGetPrinterList, and (4) XpQueryScreens functions.	libxp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424712
8002	CVE-2013-2061	Low		The openvpn_decrypt function in crypto.c in OpenVPN 2.3.0 and earlier, when running in UPD mode, allows remote attackers to obtain sensitive information via a timing attack involving an HMAC comparison function that does not run in constant time and a padding oracle attack on the CBC mode cipher.	openvpn	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445850
8003	CVE-2013-2058	Medium		The host_start function in drivers/usb/chipidea/host.c in the Linux kernel before 3.7.4 does not properly support a certain non-streaming option, which allows local users to cause a denial of service (system crash) by sending a large amount of network traffic through a USB/Ethernet adapter.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00444035
8004	CVE-2013-2055	Medium		Unspecified vulnerability in Apache Wicket 1.4.x before 1.4.23, 1.5.x before 1.5.11, and 6.x before 6.8.0 allows remote attackers to obtain sensitive information via vectors that cause raw HTML templates to be rendered without being processed and reading the information that is outside of wicket:panel markup.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6778

	A	B	C	D	E	F	G	H	I	J	K	L	M
8005	CVE-2013-2054	Medium		Buffer overflow in the atodn function in strongSwan 2.0.0 through 4.3.4, when Opportunistic Encryption is enabled and an RSA key is being used, allows remote attackers to cause a denial of service (pluto IKE daemon crash) and possibly execute arbitrary code via crafted DNS TXT records. NOTE: this might be the same vulnerability as CVE-2013-2053 and CVE-2013-2054.	strongswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426597
8006	CVE-2013-2053	Medium		Buffer overflow in the atodn function in Openswan before 2.6.39, when Opportunistic Encryption is enabled and an RSA key is being used, allows remote attackers to cause a denial of service (pluto IKE daemon crash) and possibly execute arbitrary code via crafted DNS TXT records. NOTE: this might be the same vulnerability as CVE-2013-2052 and CVE-2013-2054.	openswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426601
8007	CVE-2013-2030	Low		keystone/middleware/auth_token.py in OpenStack Nova Folsom, Grizzly, and Havana uses an insecure temporary directory for storing signing certificates, which allows local users to spoof servers by pre-creating this directory, which is reused by Nova, as demonstrated using /tmp/keystone-signing-nova on Fedora.	Openstack ceilometer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1515
8008	CVE-2013-2029	Medium		nagios.upgrade_to_v3.sh, as distributed by Red Hat and possibly others for Nagios Core 3.4.4, 3.5.1, and earlier, allows local users to overwrite arbitrary files via a symlink attack on a temporary nagioscfg file with a predictable name in /tmp/.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445877
8009	CVE-2013-2017	High		The veth (aka virtual Ethernet) driver in the Linux kernel before 2.6.34 does not properly manage skbs during congestion, which allows remote attackers to cause a denial of service (system crash) by leveraging lack of skb consumption in conjunction with a double-free error.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417559
8010	CVE-2013-2015	Medium		The ext4_orphan_del function in fs/ext4/namei.c in the Linux kernel before 3.7.3 does not properly handle orphan-list entries for non-journal filesystems, which allows physically proximate attackers to cause a denial of service (system hang) via a crafted filesystem on removable media, as demonstrated by the e2fsprogs tests/f_orphan_extents_inode/image.gz test.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415954
8011	CVE-2013-2014	Medium		OpenStack Identity (Keystone) before 2013.1 allows remote attackers to cause a denial of service (memory consumption and crash) via multiple long requests.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1935
8012	CVE-2013-2007	Medium		The qemu guest agent in Qemu 1.4.1 and earlier, as used by Xen, when started in daemon mode, uses weak permissions for certain files, which allows local users to read and write to these files.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00419900
8013	CVE-2013-2005	Medium		X.org libXt 1.1.3 and earlier does not check the return value of the XGetWindowProperty function, which allows X servers to trigger use of an uninitialized pointer and memory corruption via vectors related to the (1) ReqCleanup, (2) HandleSelectionEvents, (3) ReqTimedOut, (4) HandleNormal, and (5) HandleSelectionReplies functions.	libxt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424722
8014	CVE-2013-2004	Medium		The (1) GetDatabase and (2) _XimParseStringFile functions in X.org libX11 1.5.99.901 (1.6 RC1) and earlier do not restrict the recursion depth when processing directives to include files, which allows X servers to cause a denial of service (stack consumption) via a crafted file.	libx11	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424713
8015	CVE-2013-2003	Medium		Integer overflow in X.org libXcursor 1.1.13 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the _XcursorFileHeaderCreate function.	libxcursor	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424703
8016	CVE-2013-2002	Medium		Buffer overflow in X.org libXt 1.1.3 and earlier allows X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the _XtResourceConfigurationEH function.	libxt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424732
8017	CVE-2013-2001	Medium		Buffer overflow in X.org libXxf86vm 1.1.2 and earlier allows X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the XF86VidModeGetGammaRamp function.	libxxf86vm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424724
8018	CVE-2013-2000	Medium		Multiple buffer overflows in X.org libXxf86dga 1.1.3 and earlier allow X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the (1) XDGAQueryModes and (2) XDGASetMode functions.	libxxf86dga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424717
8019	CVE-2013-1999	Medium		Buffer overflow in X.org libXvMC 1.0.7 and earlier allows X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the XvMCGetDRInfo function.	libxvmc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424731
8020	CVE-2013-1998	Medium		Multiple buffer overflows in X.org libXi 1.7.1 and earlier allow X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the (1) XGetDeviceButtonMapping, (2) XIPassiveGrabDevice, and (3) XQueryDeviceState functions.	libxi	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424725
8021	CVE-2013-1997	Medium		Multiple buffer overflows in X.org libX11 1.5.99.901 (1.6 RC1) and earlier allow X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the (1) XAllocColorCells, (2) _XkbReadGetDeviceInfoReply, (3) _XkbReadGeomShapes, (4) _XkbReadGetGeometryReply, (5) _XkbReadKeySyms, (6) _XkbReadKeyActions, (7) _XkbReadKeyBehaviors, (8) _XkbReadModifierMap, (9) _XkbReadExplicitComponents, (10) _XkbReadVirtualModMap, (11) _XkbReadGetNamesReply, (12) _XkbReadGetMapReply, (13) _XimXGetReadData, (14) XListFonts, (15) XListExtensions, and (16) XGetFontPath functions.	libx11	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424716

	A	B	C	D	E	F	G	H	I	J	K	L	M
8022	CVE-2013-1995	Medium		X.org libXi 1.7.1 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to an unexpected sign extension in the XListInputDevices function.	libxi	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424727
8023	CVE-2013-1993	Medium		Multiple integer overflows in X.org libGLX in Mesa 9.1.1 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XF86DRIOpenConnection and (2) XF86DRIGetClientDriverName functions.	mesa	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424714
8024	CVE-2013-1992	Medium		Multiple integer overflows in X.org libdmx 1.1.2 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) DMXGetScreenAttributes, (2) DMXGetWindowAttributes, and (3) DMXGetInputAttributes functions.	libdmx	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424705
8025	CVE-2013-1991	Medium		Multiple integer overflows in X.org libXxf86dga 1.1.3 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XDGAQueryModes and (2) XDGASetMode functions.	libxxf86dga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424706
8026	CVE-2013-1990	Medium		Multiple integer overflows in X.org libXvMC 1.0.7 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XvMCListSurfaceTypes and (2) XvMCListSubpictureTypes functions.	libxvmc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424728
8027	CVE-2013-1989	Medium		Multiple integer overflows in X.org libXv 1.0.7 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XvQueryPortAttributes, (2) XvListImageFormats, and (3) XvCreateImage function.	libxv	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424730
8028	CVE-2013-1988	Medium		Multiple integer overflows in X.org libXRes 1.0.6 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XResQueryClients and (2) XResQueryClientResources functions.	libxres	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424723
8029	CVE-2013-1987	Medium		Multiple integer overflows in X.org libXrender 0.9.7 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XRenderQueryFilters, (2) XRenderQueryFormats, and (3) XRenderQueryPictIndexValues functions.	libxrender	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424719
8030	CVE-2013-1986	Medium		Multiple integer overflows in X.org libXrandr 1.4.0 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XRRQueryOutputProperty and (2) XRRQueryProviderProperty functions.	libxrandr	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424711
8031	CVE-2013-1985	Medium		Integer overflow in X.org libXinerama 1.1.2 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the XineramaQueryScreens function.	libxinerama	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424726
8032	CVE-2013-1984	Medium		Multiple integer overflows in X.org libXi 1.7.1 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XGetDeviceControl, (2) XGetFeedbackControl, (3) XGetDeviceDontPropagateList, (4) XGetDeviceMotionEvents, (5) XIGetProperty, (6) XIGetSelectedEvents, (7) XGetDeviceProperties, and (8) XListInputDevices functions.	libxi	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424721
8033	CVE-2013-1983	Medium		Integer overflow in X.org libXfixes 5.0 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the XFixesGetCursorImage function.	libxfixes	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424715
8034	CVE-2013-1982	Medium		Multiple integer overflows in X.org libXext 1.3.1 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XcupGetReservedColormapEntries, (2) XcupStoreColors, (3) XdbeGetVisualInfo, (4) XeviGetVisualInfo, (5) XShapeGetRectangles, and (6) XSyncListSystemCounters functions.	libxext	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424707
8035	CVE-2013-1981	Medium		Multiple integer overflows in X.org libX11 1.5.99.901 (1.6 RC1) and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XQueryFont, (2) _XF86BigfontQueryFont, (3) XListFontsWithInfo, (4) XGetMotionEvents, (5) XListHosts, (6) XGetModifierMapping, (7) XGetPointerMapping, (8) XGetKeyboardMapping, (9) XGetWindowProperty, (10) XGetImage, (11) LoadColornameDB, (12) XrmGetFileDatabase, (13) _XimParseStringFile, or (14) TransFileName functions.	libx11	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00424709
8036	CVE-2013-1979	Medium		The scm_set_cred function in include/net/scm.h in the Linux kernel before 3.8.11 uses incorrect uid and gid values during credentials passing, which allows local users to gain privileges via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417554
8037	CVE-2013-1969	High		Multiple use-after-free vulnerabilities in libxml2 2.9.0 and possibly other versions might allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to the (1) htmlParseChunk and (2) xmldecl_done functions, as demonstrated by a buffer overflow in the xmlBufGetInputBase function.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415969
8038	CVE-2013-1968	Medium		Subversion before 1.6.23 and 1.7.x before 1.7.10 allows remote authenticated users to cause a denial of service (FSFS repository corruption) via a newline character in a file name.	Subversion	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430969
8039	CVE-2013-1966	High		Apache Struts 2 before 2.3.14.1 allows remote attackers to execute arbitrary OGNL code via a crafted request that is not properly handled when using the includeParams attribute in the (1) URL or (2) A tag.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426600

	A	B	C	D	E	F	G	H	I	J	K	L	M
8040	CVE-2013-1965	Medium		Apache Struts Showcase App 2.0.0 through 2.3.13, as used in Struts 2 before 2.3.14.1, allows remote attackers to execute arbitrary OGNL code via a crafted parameter name that is not properly handled when invoking a redirect.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426594
8041	CVE-2013-1962	Medium		The remoteDispatchStoragePoolListAllVolumes function in the storage pool manager in libvirt 1.0.5 allows remote attackers to cause a denial of service (file descriptor consumption) via a large number of requests to list all volumes for the particular pool.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00419899
8042	CVE-2013-1961	High		Stack-based buffer overflow in the t2p_write_pdf_page function in tiff2pdf in libtiff before 4.0.3 allows remote attackers to cause a denial of service (application crash) via a crafted image length and resolution in a TIFF image file.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426596
8043	CVE-2013-1960	High		Heap-based buffer overflow in the tp_process_jpeg_strip function in tiff2pdf in libtiff 4.0.3 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted TIFF image file.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426614
8044	CVE-2013-1959	Low		kernel/user_namespace.c in the Linux kernel before 3.8.9 does not have appropriate capability requirements for the uid_map and gid_map files, which allows local users to gain privileges by opening a file within an unprivileged process and then modifying the file within a privileged process.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417550
8045	CVE-2013-1958	Medium		The scm_check_creds function in net/core/scm.c in the Linux kernel before 3.8.6 does not properly enforce capability requirements for controlling the PID value associated with a UNIX domain socket, which allows local users to bypass intended access restrictions by leveraging the time interval during which a user namespace has been created but a PID namespace has not been created.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415970
8046	CVE-2013-1957	Medium		The clone_mnt function in fs/namespace.c in the Linux kernel before 3.8.6 does not properly restrict changes to the MNT_READONLY flag, which allows local users to bypass an intended read-only property of a filesystem by leveraging a separate mount namespace.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415955
8047	CVE-2013-1955	Medium		Multiple cross-site scripting (XSS) vulnerabilities in (1) index.php and (2) datePicker.php in Easy PHP Calendar 6.x and 7.x before 7.0.13 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428873
8048	CVE-2013-1950	Medium		The svc_dg_getargs function in libtirpc 0.2.3 and earlier allows remote attackers to cause a denial of service (rpcbind crash) via a Sun RPC request with crafted arguments that trigger a free of an invalid pointer.	libtirpc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426611
8049	CVE-2013-1944	Medium		The tailMatch function in cookie.c in cURL and libcurl before 7.30.0 does not properly match the path domain when sending cookies, which allows remote attackers to steal cookies via a matching suffix in the domain of a URL.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415960
8050	CVE-2013-1943	Medium		The KVM subsystem in the Linux kernel before 3.0 does not check whether kernel addresses are specified during allocation of memory slots for use in a guest's physical address space, which allows local users to gain privileges or obtain sensitive information from kernel memory via a crafted application, related to arch/x86/kvm/paging_tmpl.h and virt/kvm/kvm_main.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428867
8051	CVE-2013-1940	Low		X.Org X server before 1.13.4 and 1.4.x before 1.14.1 does not properly restrict access to input events when adding a new hot-plug device, which might allow physically proximate attackers to obtain sensitive information, as demonstrated by reading passwords from a tty.	x.org-xserver	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00419902
8052	CVE-2013-1937	Medium		Multiple cross-site scripting (XSS) vulnerabilities in tbl_gis_visualization.php in phpMyAdmin 3.5.x before 3.5.8 might allow remote attackers to inject arbitrary web script or HTML via the (1) visualizationSettings[width] or (2) visualizationSettings[height] parameter.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415921
8053	CVE-2013-1929	Medium		Heap-based buffer overflow in the tg3_read_vpd function in drivers/net/ethernet/broadcom/tg3.c in the Linux kernel before 3.8.6 allows physically proximate attackers to cause a denial of service (system crash) or possibly execute arbitrary code via crafted firmware that specifies a long string in the Vital Product Data (VPD) data structure.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421925
8054	CVE-2013-1928	Medium		The do_video_set_spu_palette function in fs/compat_ioctl.c in the Linux kernel before 3.6.5 on unspecified architectures lacks a certain error check, which might allow local users to obtain sensitive information from kernel stack memory via a crafted VIDEO_SET_SPU_PALETTE ioctl call on a /dev/dvb device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415940
8055	CVE-2013-1923	Low		rpc-gssd in nfs-utils before 1.2.8 performs reverse DNS resolution for server names during GSSAPI authentication, which might allow remote attackers to read otherwise-restricted files via DNS spoofing attacks.	nfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6718
8056	CVE-2013-1914	Medium		Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in GNU C Library (aka glibc or libc6) 2.17 and earlier allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers a large number of domain conversion results.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415910
8057	CVE-2013-1909	Medium		The Python client in Apache Qpid before 2.2 does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433031

	A	B	C	D	E	F	G	H	I	J	K	L	M
8058	CVE-2013-1903	High		PostgreSQL, possibly 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, 8.4.x before 8.4.17, and 8.3.x before 8.3.23 incorrectly provides the superuser password to scripts related to graphical installers for Linux and Mac OS X, which has unspecified impact and attack vectors.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413554
8059	CVE-2013-1902	High		PostgreSQL, 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, 8.4.x before 8.4.17, and 8.3.x before 8.3.23 generates insecure temporary files with predictable filenames, which has unspecified impact and attack vectors related to graphical installers for Linux and Mac OS X.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413573
8060	CVE-2013-1901	Medium		PostgreSQL 9.2.x before 9.2.4 and 9.1.x before 9.1.9 does not properly check REPLICATION privileges, which allows remote authenticated users to bypass intended backup restrictions by calling the (1) pg_start_backup or (2) pg_stop_backup functions.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413565
8061	CVE-2013-1900	High		PostgreSQL 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, and 8.4.x before 8.4.17, when using OpenSSL, generates insufficiently random numbers, which might allow remote authenticated users to have an unspecified impact via vectors related to the contrib/pgcrypto functions.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413548
8062	CVE-2013-1899	Medium		Argument injection vulnerability in PostgreSQL 9.2.x before 9.2.4, 9.1.x before 9.1.9, and 9.0.x before 9.0.13 allows remote attackers to cause a denial of service (file corruption), and allows remote authenticated users to modify configuration settings and execute arbitrary code, via a connection request using a database name that begins with a - (hyphen).	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413546
8063	CVE-2013-1896	Medium		mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426612
8064	CVE-2013-1884	Medium		The mod_dav_svn Apache HTTPD server module in Subversion 1.7.0 through 1.7.8 allows remote attackers to cause a denial of service (segmentation fault and crash) via a log REPORT request with an invalid limit, which triggers an access of an uninitialized variable.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417558
8065	CVE-2013-1881	Medium		GNOME libsvg before 2.39.0 allows remote attackers to read arbitrary files via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.	librsvg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439205
8066	CVE-2013-1880	Medium		Cross-site scripting (XSS) vulnerability in the Portfolio publisher servlet in the demo web application in Apache ActiveMQ before 5.9.0 allows remote attackers to inject arbitrary web script or HTML via the refresh parameter to demo/portfolioPublish, a different vulnerability than CVE-2012-6092.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6769
8067	CVE-2013-1879	Medium		Cross-site scripting (XSS) vulnerability in scheduled.jsp in Apache ActiveMQ 5.8.0 and earlier allows remote attackers to inject arbitrary web script or HTML via vectors involving the cron of a message.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00428868
8068	CVE-2013-1872	Medium		The Intel drivers in Mesa 8.0.x and 9.0.x allow context-dependent attackers to cause a denial of service (reachable assertion and crash) and possibly execute arbitrary code via vectors involving 3d graphics that trigger an out-of-bounds array access, related to the fs_visitor::remove_dead_constants function. NOTE: this issue might be related to CVE-2013-0796.	mesa	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433024
8069	CVE-2013-1863	Medium		Samba 4.x before 4.0.4, when configured as an Active Directory domain controller, uses world-writable permissions on non-default CIFS shares, which allows remote authenticated users to read, modify, create, or delete arbitrary files via standard filesystem operations.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411212
8070	CVE-2013-1862	Medium		mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421920
8071	CVE-2013-1860	Medium		Heap-based buffer overflow in the wdm_in_callback function in drivers/usb/class/cdc-wdm.c in the Linux kernel before 3.8.4 allows physically proximate attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a crafted cdc-wdm USB device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411219
8072	CVE-2013-1858	High		The clone system-call implementation in the Linux kernel before 3.8.3 does not properly handle a combination of the CLONE_NEWUSER and CLONE_FS flags, which allows local users to gain privileges by calling chroot and leveraging the sharing of the / directory between a parent process and a child process.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413563
8073	CVE-2013-1849	Medium		The mod_dav_svn Apache HTTPD server module in Subversion 1.6.x through 1.6.20 and 1.7.0 through 1.7.8 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a PROPFIND request for an activity URL.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417552
8074	CVE-2013-1848	Medium		fs/ext3/super.c in the Linux kernel before 3.8.4 uses incorrect arguments to functions in certain circumstances related to printk input, which allows local users to conduct format-string attacks and possibly gain privileges via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411199

	A	B	C	D	E	F	G	H	I	J	K	L	M
8075	CVE-2013-1847	Medium		The mod_dav_svn Apache HTTPD server module in Subversion 1.6.0 through 1.6.20 and 1.7.0 through 1.7.8 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via an anonymous LOCK for a URL that does not exist.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417556
8076	CVE-2013-1846	Medium		The mod_dav_svn Apache HTTPD server module in Subversion 1.6.x before 1.6.21 and 1.7.0 through 1.7.8 allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via a LOCK on an activity URL.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417555
8077	CVE-2013-1845	Low		The mod_dav_svn Apache HTTPD server module in Subversion 1.6.x before 1.6.21 and 1.7.0 through 1.7.8 allows remote authenticated users to cause a denial of service (memory consumption) by (1) setting or (2) deleting a large number of properties for a file or directory.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417553
8078	CVE-2013-1828	Medium		The sctp_getsockopt_assoc_stats function in net/sctp/socket.c in the Linux kernel before 3.8.4 does not validate a size value before proceeding to a copy_from_user operation, which allows local users to gain privileges via a crafted application that contains an SCTP_GET_ASSOC_STATS getsockopt system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411217
8079	CVE-2013-1827	Medium		net/dccp/ccid.h in the Linux kernel before 3.5.4 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) by leveraging the CAP_NET_ADMIN capability for a certain (1) sender or (2) receiver getsockopt call.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411221
8080	CVE-2013-1826	Medium		The xfrm_state_netlink function in net/xfrm/xfrm_user.c in the Linux kernel before 3.5.7 does not properly handle error conditions in dump_one_state function calls, which allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) by leveraging the CAP_NET_ADMIN capability.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411202
8081	CVE-2013-1824	Medium		The SOAP parser in PHP before 5.3.22 and 5.4.x before 5.4.12 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439200
8082	CVE-2013-1821	Medium		lib/rexml/text.rb in the REXML parser in Ruby before 1.9.3-p392 allows remote attackers to cause a denial of service (memory consumption and crash) via crafted text nodes in an XML document, aka an XML Entity Expansion (XEE) attack.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413569
8083	CVE-2013-1819	Medium		The _xfs_buf_find function in fs/xfs/xfs_buf.c in the Linux kernel before 3.7.6 does not validate block numbers, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by leveraging the ability to mount an XFS filesystem containing a metadata inode with an invalid extent map.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408772
8084	CVE-2013-1813	High		util-linux/mdev.c in BusyBox before 1.21.0 uses 0777 permissions for parent directories when creating nested directories under /dev/, which allows local users to have unknown impact and attack vectors.	busybox	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445880
8085	CVE-2013-1812	Medium		The ruby-openid gem before 2.2.2 for Ruby allows remote OpenID providers to cause a denial of service (CPU consumption) via (1) a large XRDS document or (2) an XML Entity Expansion (XEE) attack.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448726
8086	CVE-2013-1798	Medium		The ioapic_read_indirect function in virt/kvm/ioapic.c in the Linux kernel through 3.8.4 does not properly handle a certain combination of invalid IOAPIC_REG_SELECT and IOAPIC_REG_WINDOW operations, which allows guest OS users to obtain sensitive information from host OS memory or cause a denial of service (host OS OOPS) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411203
8087	CVE-2013-1797	Medium		Use-after-free vulnerability in arch/x86/kvm/x86.c in the Linux kernel through 3.8.4 allows guest OS users to cause a denial of service (host OS memory corruption) or possibly have unspecified other impact via a crafted application that triggers use of a guest physical address (GPA) in (1) movable or (2) removable memory during an MSR_KVM_SYSTEM_TIME kvm_set_msr_common operation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411216
8088	CVE-2013-1796	Medium		The kvm_set_msr_common function in arch/x86/kvm/x86.c in the Linux kernel through 3.8.4 does not ensure a required time_page alignment during an MSR_KVM_SYSTEM_TIME operation, which allows guest OS users to cause a denial of service (buffer overflow and host OS memory corruption) or possibly have unspecified other impact via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411210
8089	CVE-2013-1792	Medium		Race condition in the install_user_keyrings function in security/keys/process_keys.c in the Linux kernel before 3.8.3 allows local users to cause a denial of service (NULL pointer dereference and system crash) via crafted keyctl system calls that trigger keyring operations in simultaneous threads.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411211
8090	CVE-2013-1790	Medium		poppler/Stream.cc in poppler before 0.22.1 allows context-dependent attackers to have an unspecified impact via vectors that trigger a read of uninitialized memory by the CCITTFaxStream::lookChar function.	poppler	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413545

	A	B	C	D	E	F	G	H	I	J	K	L	M
8091	CVE-2013-1789	Medium		splash/Splash.cc in poppler before 0.22.1 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to the (1) Splash::arbitraryTransformMask, (2) Splash::blitMask, and (3) Splash::scaleMaskYuXu functions.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	poppler	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413577
8092	CVE-2013-1788	Medium		poppler before 0.22.1 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors that trigger an invalid memory access in (1) splash/Splash.cc, (2) poppler/Function.cc, and (3) poppler/Stream.cc.	poppler	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413556
8093	CVE-2013-1777	High		The JMX Remoting functionality in Apache Geronimo 3.x before 3.0.1, as used in IBM WebSphere Application Server (WAS) Community Edition 3.0.0.3 and other products, does not property implement the RMI classloader, which allows remote attackers to execute arbitrary code by using the JMX connector to send a crafted serialized object.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426595
8094	CVE-2013-1776	Medium		sudo 1.3.5 through 1.7.10 and 1.8.0 through 1.8.5, when the tty_tickets option is enabled, does not properly validate the controlling terminal device, which allows local users with sudo permissions to hijack the authorization of another terminal via vectors related to connecting to a standard input, output, and error file descriptors of another terminal. NOTE: this is one of three closely-related vulnerabilities that were originally assigned CVE-2013-1776, but they have been SPLIT because of different affected versions.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413581
8095	CVE-2013-1775	Medium		sudo 1.6.0 through 1.7.10p6 and sudo 1.8.0 through 1.8.6p6 allows local users or physically-proximate attackers to bypass intended time restrictions and retain privileges without re-authenticating by setting the system clock and sudo user timestamp to the epoch.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408774
8096	CVE-2013-1774	Medium		The chase_port function in drivers/usb/serial/io_ti.c in the Linux kernel before 3.7.4 allows local users to cause a denial of service (NULL pointer dereference and system crash) via an attempted /dev/ttyUSB read or write operation on a disconnected Edgeport USB serial converter.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406215
8097	CVE-2013-1773	Medium		Buffer overflow in the VFAT filesystem implementation in the Linux kernel before 3.3 allows local users to gain privileges or cause a denial of service (system crash) via a VFAT write operation on a filesystem with the utf8 mount option, which is not properly handled during UTF-8 to UTF-16 conversion.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406212
8098	CVE-2013-1772	Medium		The log_prefix function in kernel/printk.c in the Linux kernel 3.x before 3.4.33 does not properly remove a prefix string from a syslog header, which allows local users to cause a denial of service (buffer overflow and system crash) by leveraging /dev/kmsg write access and triggering a call_console_drivers function call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406220
8099	CVE-2013-1768	High		The BrokerFactory functionality in Apache OpenJPA 1.x before 1.2.3 and 2.x before 2.2.2 creates local executable JSP files containing logging trace data produced during deserialization of certain crafted OpenJPA objects, which makes it easier for remote attackers to execute arbitrary code by creating a serialized object and leveraging improperly secured server programs.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426608
8100	CVE-2013-1767	Medium		Use-after-free vulnerability in the shmem_remount_fs function in mm/shmem.c in the Linux kernel before 3.7.10 allows local users to gain privileges or cause a denial of service (system crash) by remounting a tmpfs filesystem without specifying a required mpol (aka mempolicy) mount option.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406208
8101	CVE-2013-1766	Low		libvirt 1.0.2 and earlier sets the group owner to kvm for device files, which allows local users to write to these files via unspecified vectors.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411208
8102	CVE-2013-1763	High		Array index error in the __sock_diag_rcv_msg function in net/core/sock_diag.c in the Linux kernel before 3.7.10 allows local users to gain privileges via a large family value in a Netlink message.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406214
8103	CVE-2013-1749	Medium		Cross-site scripting (XSS) vulnerability in edit.php in PHP Address Book 8.2.5 allows user-assisted remote attackers to inject arbitrary web script or HTML via the Address field.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415926
8104	CVE-2013-1748	High		Multiple SQL injection vulnerabilities in PHP Address Book 8.2.5 allow remote attackers to execute arbitrary SQL commands via unspecified parameters to (1) edit.php or (2) import.php. NOTE: the view.php id vector is already covered by CVE-2008-2565.1 and the edit.php id vector is already covered by CVE-2008-2565.2.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415939
8105	CVE-2013-1741	High		Integer overflow in Mozilla Network Security Services (NSS) 3.15 before 3.15.3 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large size value.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445876
8106	CVE-2013-1740	Medium		The ssl_Do1stHandshake function in sslsecur.c in libssl in Mozilla Network Security Services (NSS) before 3.15.4, when the TLS False Start feature is enabled, allows man-in-the-middle attackers to spoof SSL servers by using an arbitrary X.509 certificate during certain handshake traffic.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6725
8107	CVE-2013-1739	Medium		Mozilla Network Security Services (NSS) before 3.15.2 does not ensure that data structures are initialized before read operations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a decryption failure.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441882
8108	CVE-2013-1667	High		The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413550

	A	B	C	D	E	F	G	H	I	J	K	L	M
8109	CVE-2013-1643	Medium		The SOAP parser in PHP before 5.3.22 and 5.4.x before 5.4.13 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408769
8110	CVE-2013-1635	High		ext/soap/soap.c in PHP before 5.3.22 and 5.4.x before 5.4.13 does not validate the relationship between the soap.wsdl_cache_dir directive and the open_basedir directive, which allows remote attackers to bypass intended access restrictions by triggering the creation of cached SOAP WSDL files in an arbitrary directory.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408770
8111	CVE-2013-1620	High		The TLS implementation in Mozilla Network Security Services (NSS) does not properly consider timing side-channel attacks on a noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411215
8112	CVE-2013-1619	Medium		The TLS implementation in GnuTLS before 2.12.23, 3.0.x before 3.0.28, and 3.1.x before 3.1.7 does not properly consider timing side-channel attacks on a noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404151
8113	CVE-2013-1570	Medium		Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote attackers to affect availability via unknown vectors related to MemCached.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415942
8114	CVE-2013-1567	Low		Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language, a different vulnerability than CVE-2013-2395.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415948
8115	CVE-2013-1566	Low		Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415935
8116	CVE-2013-1555	Medium		Unspecified vulnerability in MySQL 5.1.67 and earlier and 5.5.29 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415966
8117	CVE-2013-1552	Medium		Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier and 5.5.29 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415913
8118	CVE-2013-1548	Low		Unspecified vulnerability in Oracle MySQL 5.1.63 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Types.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415928
8119	CVE-2013-1544	Medium		Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415924
8120	CVE-2013-1532	Medium		Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Information Schema.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415912
8121	CVE-2013-1531	Medium		Unspecified vulnerability in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Server Privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415931
8122	CVE-2013-1526	Medium		Unspecified vulnerability in Oracle MySQL 5.5.29 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415961
8123	CVE-2013-1523	Medium		Unspecified vulnerability in Oracle MySQL 5.5.29 and earlier and 5.6.10 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415972
8124	CVE-2013-1521	Medium		Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier and 5.5.29 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Server Locking.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415920
8125	CVE-2013-1512	Medium		Unspecified vulnerability in Oracle MySQL 5.5.29 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415932
8126	CVE-2013-1511	Low		Unspecified vulnerability in Oracle MySQL 5.5.30 and earlier and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415943
8127	CVE-2013-1506	Low		Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier, 5.5.29 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Locking.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415944
8128	CVE-2013-1502	Low		Unspecified vulnerability in Oracle MySQL 5.5.30 and earlier and 5.6.9 and earlier allows local users to affect availability via unknown vectors related to Server Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415956
8129	CVE-2013-1492	High		Buffer overflow in yaSSL, as used in MySQL 5.1.x before 5.1.68 and 5.5.x before 5.5.30, has unspecified impact and attack vectors, a different vulnerability than CVE-2012-0553.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413586

	A	B	C	D	E	F	G	H	I	J	K	L	M
8130	CVE-2013-1427	Low		The configuration file for the FastCGI PHP support for lighthttpd before 1.4.28 on Debian GNU/Linux creates a socket file with a predictable name in /tmp, which allows local users to hijack the PHP control socket and perform unauthorized actions such as forcing the use of a different version of PHP via a symlink attack or a race condition.	lighttpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445842
8131	CVE-2013-1418	Medium		The setup_server_realm function in main.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.10.7, when multiple realms are configured, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted request.CWE-476: NULL Pointer Dereference per http://cwe.mitre.org/data/definitions/476.html	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445846
8132	CVE-2013-1417	Low		do_tgs_req.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.11 before 1.11.4, when a single-component realm name is used, allows remote authenticated users to cause a denial of service (daemon crash) via a TGS-REQ request that triggers an attempted cross-realm referral for a host-based service principal.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445865
8133	CVE-2013-1416	Medium		The prep_reprocess_req function in do_tgs_req.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.10.5 does not properly perform service-principal realm referral, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted TGS-REQ request.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415916
8134	CVE-2013-1415	High		The pkinit_check_kdc_pkid function in plugins/preauth/pkinit/pkinit_crypto_openssl.c in the PKINIT implementation in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.10.4 and 1.11.x before 1.11.1 does not properly handle errors during extraction of fields from an X.509 certificate, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a malformed KRB5_PADATA_PK_AS_REQ AS-REQ request.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413555
8135	CVE-2013-1068	Medium		The OpenStack Nova (python-nova) package 1:2013.2.3-0 before 1:2013.2.3-0ubuntu1.2 and 1:2014.1-0 before 1:2014.1-0ubuntu1.2 and Openstack Cinder (python-cinder) package 1:2013.2.3-0 before 1:2013.2.3-0ubuntu1.1 and 1:2014.1-0 before 1:2014.1-0ubuntu1.1 for Ubuntu 13.10 and 14.04 LTS does not properly set the sudo configuration, which makes it easier for attackers to gain privileges by leveraging another vulnerability.	openstack	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1958
8136	CVE-2013-1059	High		net/ceph/auth_none.c in the Linux kernel through 3.10 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via an auth_reply message that triggers an attempted build_request operation.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00426605
8137	CVE-2013-1056	Low		X.org X server 1.13.3 and earlier, when not run as root, allows local users to cause a denial of service (crash) or possibly gain privileges via vectors involving cached xkb files.	X.org	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00441889
8138	CVE-2013-1051	Medium		apt 0.8.16, 0.9.7, and possibly other versions does not properly handle InRelease files, which allows man-in-the-middle attackers to modify packages before installation via unknown vectors, possibly related to integrity checking and the use of third-party repositories.	apt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411348
8139	CVE-2013-1048	Medium		The Debian apache2ctl script in the apache2 package squeeze before 2.2.16-6+squeeze11, wheezy before 2.2.22-13, and sid before 2.2.22-13 for the Apache HTTP Server on Debian GNU/Linux does not properly create the /var/lock/apache2 lock directory, which allows local users to gain privileges via an unspecified symlink attack.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408763
8140	CVE-2013-0913	High		Integer overflow in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the i915 driver in the Direct Rendering Manager (DRM) subsystem in the Linux kernel through 3.8.3, as used in Google Chrome OS before 25.0.1364.173 and other products, allows local users to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted application that triggers many relocation copies, and potentially leads to a race condition.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411201
8141	CVE-2013-0900	Medium		Race condition in the International Components for Unicode (ICU) functionality in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.	icu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00443085
8142	CVE-2013-0878	High		The advance_line function in libavcodec/targa.c in FFmpeg before 1.1.3 allows remote attackers to have an unspecified impact via crafted Targa image data, related to an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445845
8143	CVE-2013-0877	High		The old_codec37 function in libavcodec/sanm.c in FFmpeg before 1.1.3 allows remote attackers to have an unspecified impact via crafted LucasArts Smush data that has a large size when decoded, related to an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445856
8144	CVE-2013-0876	High		Multiple integer overflows in the (1) old_codec37 and (2) old_codec47 functions in libavcodec/sanm.c in FFmpeg before 1.1.3 allow remote attackers to have an unspecified impact via crafted LucasArts Smush data, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445871

	A	B	C	D	E	F	G	H	I	J	K	L	M
8145	CVE-2013-0875	High		The ff_add_png_paeth_prediction function in libavcodec/pngdec.c in FFmpeg before 1.1.3 allows remote attackers to have an unspecified impact via a crafted PNG image, related to an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445837
8146	CVE-2013-0874	High		The (1) doubles2str and (2) shorts2str functions in libavcodec/tiff.c in FFmpeg before 1.1.3 allow remote attackers to have an unspecified impact via a crafted TIFF image, related to an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445855
8147	CVE-2013-0873	High		The read_header function in libavcodec/shorten.c in FFmpeg before 1.1.3 allows remote attackers to have an unspecified impact via an invalid channel count, related to freeing invalid addresses.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445862
8148	CVE-2013-0872	High		The swr_init function in libswresample/swresample.c in FFmpeg before 1.1.3 allows remote attackers to have an unspecified impact via an invalid or unsupported (1) input or (2) output channel layout, related to an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445881
8149	CVE-2013-0871	Medium		Race condition in the ptrace functionality in the Linux kernel before 3.7.5 allows local users to gain privileges via a PTRACE_SETREGS ptrace system call in a crafted application, as demonstrated by ptrace_death.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406219
8150	CVE-2013-0870	High	Critical	The 'vp3_decode_frame' function in FFmpeg 1.1.4 moves threads check out of header packet type check.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5291
8151	CVE-2013-0869	High		The field_end function in libavcodec/h264.c in FFmpeg before 1.1.2 allows remote attackers to have an unspecified impact via crafted H.264 data, related to an SPS and slice mismatch and an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445848
8152	CVE-2013-0868	High		libavcodec/huffyuvdec.c in FFmpeg before 1.1.2 allows remote attackers to have an unspecified impact via crafted Huffyuv data, related to an out-of-bounds write and (1) unchecked return codes from the init_vlc function and (2) len==0 cases.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445860
8153	CVE-2013-0867	High		The decode_slice_header function in libavcodec/h264.c in FFmpeg before 1.1.2 does not properly check when the pixel format changes, which allows remote attackers to have unspecified impact via crafted H.264 video data, related to an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445878
8154	CVE-2013-0866	High		The aac_decode_init function in libavcodec/aacdec.c in FFmpeg before 1.0.4 and 1.1.x before 1.1.2 allows remote attackers to have an unspecified impact via a large number of channels in an AAC file, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445836
8155	CVE-2013-0865	High		The vqa_decode_chunk function in libavcodec/vqavideo.c in FFmpeg before 1.0.4 and 1.1.x before 1.1.2 allows remote attackers to have an unspecified impact via a large (1) cbp0 or (2) cbpz chunk in Westwood Studios VQA Video file, which triggers an out-of-bounds write.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445840
8156	CVE-2013-0864	High		The gif_copy_img_rect function in libavcodec/gifdec.c in FFmpeg before 1.1.2 performs an incorrect calculation for an end pointer, which allows remote attackers to have an unspecified impact via crafted GIF data that triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445882
8157	CVE-2013-0863	High		Buffer overflow in the rle_decode function in libavcodec/sanm.c in FFmpeg before 1.0.4 and 1.1.x before 1.1.2 allows remote attackers to have an unspecified impact via crafted LucasArts Smush video data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445875
8158	CVE-2013-0862	High		Multiple integer overflows in the process_frame_obj function in libavcodec/sanm.c in FFmpeg before 1.1.2 allow remote attackers to have an unspecified impact via crafted image dimensions in LucasArts Smush video data, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445828
8159	CVE-2013-0861	Medium		The avcodec_decode_audio4 function in libavcodec/utils.c in FFmpeg before 1.0.4 and 1.1.x before 1.1.1 allows remote attackers to trigger memory corruption via vectors related to the channel layout.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445833
8160	CVE-2013-0860	Medium		The ff_er_frame_end function in libavcodec/error_resilience.c in FFmpeg before 1.0.4 and 1.1.x before 1.1.1 does not properly verify that a frame is fully initialized, which allows remote attackers to trigger a NULL pointer dereference via crafted picture data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445847
8161	CVE-2013-0859	High		The add_doubles_metadata function in libavcodec/tiff.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a negative or zero count value in a TIFF image, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448761
8162	CVE-2013-0858	High		The atrac3_decode_init function in libavcodec/atrac3.c in FFmpeg before 1.0.4 allows remote attackers to have an unspecified impact via ATRAC3 data with the joint stereo coding mode set and fewer than two channels.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448741
8163	CVE-2013-0857	High		The decode_frame_ilbm function in libavcodec/iff.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a crafted height value in IFF PBM/ILBM bitmap data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448734
8164	CVE-2013-0856	High		The lpc_prediction function in libavcodec/alac.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted Apple Lossless Audio Codec (ALAC) data, related to a large nb_samples value.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448747
8165	CVE-2013-0855	High		Integer overflow in the alac_decode_close function in libavcodec/alac.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a large number of samples per frame in Apple Lossless Audio Codec (ALAC) data, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448733
8166	CVE-2013-0854	High		The mjpeg_decode_scan_progressive_ac function in libavcodec/mjpegdec.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted MJPEG data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448746

	A	B	C	D	E	F	G	H	I	J	K	L	M
8167	CVE-2013-0853	High		The wavpack_decode_frame function in libavcodec/wavpack.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted WavPack data, which triggers an out-of-bounds array access, possibly due to an off-by-one error.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448771
8168	CVE-2013-0852	High		The parse_picture_segment function in libavcodec/pgssubdec.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted RLE data, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448720
8169	CVE-2013-0851	High		The decode_frame function in libavcodec/eamad.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted Electronic Arts Madcow video data, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448745
8170	CVE-2013-0850	High		The decode_slice_header function in libavcodec/h264.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted H.264 data, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448753
8171	CVE-2013-0849	High		The roq_decode_init function in libavcodec/roqvideodec.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a crafted (1) width or (2) height dimension that is not a multiple of sixteen in id RoQ video data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448755
8172	CVE-2013-0848	High		The decode_init function in libavcodec/huffyuv.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via a crafted width in huffyuv data with the predictor set to median and the colorspace set to YUV422P, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448739
8173	CVE-2013-0847	High		The ff_id3v2_parse function in libavformat/id3v2.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via ID3v2 header data, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448716
8174	CVE-2013-0846	High		Array index error in the qdm2_decode_super_block function in libavcodec/qdm2.c in FFmpeg before 1.1 allows remote attackers to have an unspecified impact via crafted QDM2 data, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448774
8175	CVE-2013-0845	High		libavcodec/alsdec.c in FFmpeg before 1.0.4 allows remote attackers to have an unspecified impact via a crafted block length, which triggers an out-of-bounds write.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448717
8176	CVE-2013-0844	High		Off-by-one error in the adpcm_decode_frame function in libavcodec/adpcm.c in FFmpeg before 1.0.4 allows remote attackers to have an unspecified impact via crafted DK4 data, which triggers an out-of-bounds array access.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448776
8177	CVE-2013-0791	Medium		The CERT_DecodeCertPackage function in Mozilla Network Security Services (NSS), as used in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, SeaMonkey before 2.17, and other products, allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) via a crafted certificate.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413575
8178	CVE-2013-0721	Medium		wp-php-widget.php in the WP PHP widget plugin 1.0.2 for WordPress allows remote attackers to obtain sensitive information via a direct request, which reveals the full path in an error message.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399169
8179	CVE-2013-0454	Medium		Samba before 3.6.6, as used on the IBM Storwize V7000 Unified 1.3 before 1.3.2.3 and 1.4 before 1.4.0.1 and possibly other products, does not properly enforce CIFS share attributes, which allows remote authenticated users to (1) write to a read-only share; (2) trigger data-integrity problems related to the oplock, locking, coherency, or leases attribute; or (3) have an unspecified impact by leveraging incorrect handling of the browseable or hide unreadable parameter.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411205
8180	CVE-2013-0389	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402364
8181	CVE-2013-0386	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to Stored Procedure.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402352
8182	CVE-2013-0385	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows local users to affect confidentiality and integrity via unknown vectors related to Server Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402369
8183	CVE-2013-0384	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Information Schema.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402379
8184	CVE-2013-0383	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows remote attackers to affect availability via unknown vectors related to Server Locking.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402350
8185	CVE-2013-0375	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.1.28 and earlier, allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Server Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402378
8186	CVE-2013-0371	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability, related to MyISAM.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402363
8187	CVE-2013-0368	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402370

	A	B	C	D	E	F	G	H	I	J	K	L	M
8188	CVE-2013-0367	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402359
8189	CVE-2013-0349	Low		The hidp_setup_hid function in net/bluetooth/hidp/core.c in the Linux kernel before 3.7.6 does not properly copy a certain name field, which allows local users to obtain sensitive information from kernel memory by setting a long name and making an HIDPCONNADD ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406225
8190	CVE-2013-0343	Low		The ipv6_create_tempaddr function in net/ipv6/addrconf.c in the Linux kernel through 3.8 does not properly handle problems with the generation of IPv6 temporary addresses, which allows remote attackers to cause a denial of service (excessive retries and address-generation outage), and consequently obtain sensitive information, via ICMPv6 Router Advertisement (RA) messages.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406216
8191	CVE-2013-0340	Medium		expat 2.1.0 and earlier does not properly handle entities expansion unless an application developer uses the XML_SetEntityDeclHandler function, which allows remote attackers to cause a denial of service (resource consumption), send HTTP requests to intranet servers, or read arbitrary files via a crafted XML document, aka an XML External Entity (XXE) issue. NOTE: it could be argued that because expat already provides the ability to disable external entity expansion, the responsibility for resolving this issue lies with application developers; according to this argument, this entry should be REJECTed, and each affected application would need its own CVE.	expat	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN6-6771
8192	CVE-2013-0339	Medium		libxml2 through 2.9.1 does not properly handle external entities expansion unless an application developer uses the xmlSAX2ResolveEntity or xmlSetExternalEntityLoader function, which allows remote attackers to cause a denial of service (resource consumption), send HTTP requests to intranet servers, or read arbitrary files via a crafted XML document, aka an XML External Entity (XXE) issue. NOTE: it could be argued that because libxml2 already provides the ability to disable external entity expansion, the responsibility for resolving this issue lies with application developers; according to this argument, this entry should be REJECTed and each affected application would need its own CVE.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6756
8193	CVE-2013-0338	Medium		libxml2 2.9.0 and earlier allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via an XML file containing an entity declaration with long replacement text and many references to this entity, aka internal entity expansion with linear complexity.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415967
8194	CVE-2013-0333	High		lib/active_support/json/backends/yaml.rb in Ruby on Rails 2.3.x before 2.3.16 and 3.0.x before 3.0.20 does not properly convert JSON data to YAML data for processing by a YAML parser, which allows remote attackers to execute arbitrary code, conduct SQL injection attacks, or bypass authentication via crafted data that triggers unsafe decoding, a different vulnerability than CVE-2013-0156.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402354
8195	CVE-2013-0313	Medium		The evm_update_evmxattr function in security/integrity/evm/evm_crypto.c in the Linux kernel before 3.7.5, when the Extended Verification Module (EVM) is enabled, allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via an attempted removexattr operation on an inode of a sockfs filesystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406218
8196	CVE-2013-0311	Medium		The translate_desc function in drivers/vhost/vhost.c in the Linux kernel before 3.7 does not properly handle cross-region descriptors, which allows guest OS users to obtain host OS privileges by leveraging KVM guest OS privileges.Per https://access.redhat.com/security/cve/CVE-2013-0311 This issue did affect the version of Linux kernel as shipped with Red Hat Enterprise Linux 6.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406228
8197	CVE-2013-0310	Medium		The cipso_v4_validate function in net/ipv4/cipso_ipv4.c in the Linux kernel before 3.4.8 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via an IPOPT_CIPSO IP_OPTIONS setsockopt system call.Per https://access.redhat.com/security/cve/CVE-2013-0310 This issue did affect the version of Linux kernel as shipped with Red Hat Enterprise Linux 6.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406227
8198	CVE-2013-0309	Medium		arch/x86/include/asm/pgtable.h in the Linux kernel before 3.6.2, when transparent huge pages are used, does not properly support PROT_NONE memory regions, which allows local users to cause a denial of service (system crash) via a crafted application.Per https://access.redhat.com/security/cve/CVE-2013-0309 This issue did affect the version of Linux kernel as shipped with Red Hat Enterprise Linux 6.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406234
8199	CVE-2013-0308	Medium		The imap-send command in GIT before 1.8.1.4 does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.	git	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413587
8200	CVE-2013-0296	Medium		Race condition in pigz before 2.2.5 uses permissions derived from the umask when compressing a file before setting that file's permissions to match those of the original file, which might allow local users to bypass intended access permissions while compression is occurring.	pigz	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7279

	A	B	C	D	E	F	G	H	I	J	K	L	M
8201	CVE-2013-0290	Medium		The __skb_recv_datagram function in net/core/datagram.c in the Linux kernel before 3.8 does not properly handle the MSG_PEEK flag with zero-length data, which allows local users to cause a denial of service (infinite loop and system hang) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406221
8202	CVE-2013-0288	Medium		nss-pam-ldapd before 0.7.18 and 0.8.x before 0.8.11 allows context-dependent attackers to cause a denial of service (application crash) and possibly execute arbitrary code by performing a name lookup on an application with a large number of open file descriptors, which triggers a stack-based buffer overflow related to incorrect use of the FD_SET macro.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408762
8203	CVE-2013-0281	Medium		Pacemaker 1.1.10, when remote Cluster Information Base (CIB) configuration or resource management is enabled, does not limit the duration of connections to the blocking sockets, which allows remote attackers to cause a denial of service (connection blocking).	pacemaker	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445852
8204	CVE-2013-0277	High		Active Record in Ruby on Rails 3.x before 3.1.0 and 2.3.x before 2.3.17 allows remote attackers to cause a denial of service or execute arbitrary code via crafted serialized attributes that cause the +serialize+ helper to deserialize arbitrary YAML.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404142
8205	CVE-2013-0276	Medium		ActiveRecord in Ruby on Rails 3.2.x before 3.2.12, 3.1.x before 3.1.11, and 2.3.x before 2.3.17 allows remote attackers to bypass the attr_protected protection mechanism and modify protected model attributes via a crafted request.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404145
8206	CVE-2013-0268	Medium		The msr_open function in arch/x86/kernel/msr.c in the Linux kernel before 3.7.6 allows local users to bypass intended capability restrictions by executing a crafted application as root, as demonstrated by msr32.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406217
8207	CVE-2013-0256	Medium		darkfish.js in RDoc 2.3.0 through 3.12 and 4.x before 4.0.0.preview2.1, as used in Ruby, does not properly generate documents, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted URL.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406236
8208	CVE-2013-0255	Medium		PostgreSQL 9.2.x before 9.2.3, 9.1.x before 9.1.8, 9.0.x before 9.0.12, 8.4.x before 8.4.16, and 8.3.x before 8.3.23 does not properly declare the enum_recv function in backend/utils/adt/enum.c, which causes it to be invoked with incorrect arguments and allows remote authenticated users to cause a denial of service (server crash) or read sensitive process memory via a crafted SQL command, which triggers an array index error and an out-of-bounds read.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404148
8209	CVE-2013-0254	Low		The QSharedMemory class in Qt 5.0.0, 4.8.x before 4.8.5, 4.7.x before 4.7.6, and other versions including 4.4.0 uses weak permissions (world-readable and world-writable) for shared memory segments, which allows local users to read sensitive information or modify critical program data, as demonstrated by reading a pixmap being sent to an X server.	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404139
8210	CVE-2013-0252	Medium		boost::locale::utf::utf_traits in the Boost.Locale library in Boost 1.48 through 1.52 does not properly detect certain invalid UTF-8 sequences, which might allow remote attackers to bypass input validation protection mechanisms via crafted trailing bytes.	boost	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413590
8211	CVE-2013-0250	Medium		The init_nss_hash function in exec/totemcrypto.c in Corosync 2.0 before 2.3 does not properly initialize the HMAC key, which allows remote attackers to cause a denial of service (crash) via a crafted packet.Per: http://cwe.mitre.org/data/definitions/665.html CWE-665: Improper Initialization	corosync	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	CGP6-475
8212	CVE-2013-0249	High		Stack-based buffer overflow in the Curl_sasl_create_digest_md5_message function in lib/curl_sasl.c in curl and libcurl 7.26.0 through 7.28.1, when negotiating SASL DIGEST-MD5 authentication, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long string in the realm parameter in a (1) POP3, (2) SMTP or (3) IMAP message.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413576
8213	CVE-2013-0242	Medium		Buffer overflow in the extend_buffers function in the regular expression matcher (posix/regexec.c) in glibc, possibly 2.17 and earlier, allows context-dependent attackers to cause a denial of service (memory corruption and crash) via crafted multibyte characters.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404152
8214	CVE-2013-0231	Medium		The pciback_enable_msi function in the PCI backend driver (drivers/xen/pciback/conf_space_capability_msi.c) in Xen for the Linux kernel 2.6.18 and 3.8 allows guest OS users with PCI device access to cause a denial of service via a large number of kernel log messages. NOTE: some of these details are obtained from third party information.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404150
8215	CVE-2013-0228	Medium		The xen_iret function in arch/x86/xen/xen-asm_32.S in the Linux kernel before 3.7.9 on 32-bit Xen paravirt_ops platforms does not properly handle an invalid value in the DS segment register, which allows guest OS users to gain guest OS privileges via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408768
8216	CVE-2013-0223	Low		The SUSE coreutils-i18n.patch for GNU coreutils allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a long string to the join command, when using the -i switch, which triggers a stack-based buffer overflow in the alloca function.	coreutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445835
8217	CVE-2013-0222	Low		The SUSE coreutils-i18n.patch for GNU coreutils allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a long string to the uniq command, which triggers a stack-based buffer overflow in the alloca function.	coreutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445854

	A	B	C	D	E	F	G	H	I	J	K	L	M
8218	CVE-2013-0221	Medium		The SUSE coreutils-i18n.patch for GNU coreutils allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a long string to the sort command, when using the (1) -d or (2) -M switch, which triggers a stack-based buffer overflow in the alloca function.	coreutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445867
8219	CVE-2013-0217	Medium		Memory leak in drivers/net/xen-netback/netback.c in the Xen netback functionality in the Linux kernel before 3.7.8 allows guest OS users to cause a denial of service (memory consumption) by triggering certain error conditions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406235
8220	CVE-2013-0216	Medium		The Xen netback functionality in the Linux kernel before 3.7.8 allows guest OS users to cause a denial of service (loop) by triggering ring pointer corruption.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406210
8221	CVE-2013-0214	Medium		Cross-site request forgery (CSRF) vulnerability in the Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.21, 3.6.x before 3.6.12, and 4.x before 4.0.2 allows remote attackers to hijack the authentication of arbitrary users by leveraging knowledge of a password and composing requests that perform SWAT actions.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404149
8222	CVE-2013-0213	Medium		The Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.21, 3.6.x before 3.6.12, and 4.x before 4.0.2 allows remote attackers to conduct clickjacking attacks via a (1) FRAME or (2) IFRAME element.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404137
8223	CVE-2013-0211	Medium		Integer signedness error in the archive_write_zip_data function in archive_write_set_format_zip.c in libarchive 3.1.2 and earlier, when running on 64-bit machines, allows context-dependent attackers to cause a denial of service (crash) via unspecified vectors, which triggers an improper conversion between unsigned and signed types, leading to a buffer overflow.	libarchive	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439179
8224	CVE-2013-0190	Medium		The xen_failsafe_callback function in Xen for the Linux kernel 2.6.23 and other versions, when running a 32-bit PVOPS guest, allows local users to cause a denial of service (guest crash) by triggering an iret fault, leading to use of an incorrect stack pointer and stack corruption.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404140
8225	CVE-2013-0176	Medium		The publickey_from_privatekey function in libssh before 0.5.4, when no algorithm is matched during negotiations, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a Client: Diffie-Hellman Key Exchange Init packet.	libssh2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404144
8226	CVE-2013-0172	Low		Samba 4.0.x before 4.0.1, in certain Active Directory domain-controller configurations, does not properly interpret Access Control Entries that are based on an objectClass, which allows remote authenticated users to bypass intended restrictions on modifying LDAP directory objects by leveraging (1) objectClass access by a user, (2) objectClass access by a group, or (3) write access to an attribute.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402362
8227	CVE-2013-0170	High		Use-after-free vulnerability in the virNetMessageFree function in rpc/virnetserverclient.c libvirt 1.0.x before 1.0.2, 0.10.2 before 0.10.2.3, 0.9.11 before 0.9.11.9, and 0.9.6 before 0.9.6.4 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by triggering certain errors during an RPC connection, which causes a message to be freed without being removed from the message queue.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404146
8228	CVE-2013-0169	Low		The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the Lucky Thirteen issue.Per http://www.openssl.org/news/vulnerabilities.html:	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404151
8229	CVE-2013-0166	Medium		OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404141
8230	CVE-2013-0162	Low		The diff_pp function in lib/gauntlet_rubyparser.rb in the ruby_parser gem 3.1.1 and earlier for Ruby allows local users to overwrite arbitrary files via a symlink attack on a temporary file with a predictable name in /tmp.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406233
8231	CVE-2013-0160	Low		The Linux kernel through 3.7.9 allows local users to obtain sensitive information about keystroke timing by using the inotify API on the /dev/ptmx device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406224
8232	CVE-2013-0157	Low		(a) mount and (b) umount in util-linux 2.14.1, 2.17.2, and probably other versions allow local users to determine the existence of restricted directories by (1) using the --guess-fstype command-line option or (2) attempting to mount a non-existent device, which generates different error messages depending on whether the directory exists.	util-linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6750
8233	CVE-2013-0156	High		active_support/core_ext/hash/conversions.rb in Ruby on Rails before 2.3.15, 3.0.x before 3.0.19, 3.1.x before 3.1.10, and 3.2.x before 3.2.11 does not properly restrict casts of string values, which allows remote attackers to conduct object-injection attacks and execute arbitrary code, or cause a denial of service (memory and CPU consumption) involving nested XML entity references, by leveraging Action Pack support for (1) YAML type conversion or (2) Symbol type conversion.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399174

	A	B	C	D	E	F	G	H	I	J	K	L	M
8234	CVE-2013-0155	High		Ruby on Rails 3.0.x before 3.0.19, 3.1.x before 3.1.10, and 3.2.x before 3.2.11 does not properly consider differences in parameter handling between the Active Record component and the JSON implementation, which allows remote attackers to bypass intended database-query restrictions and perform NULL checks or trigger missing WHERE clauses via a crafted request, as demonstrated by certain [nil] values, a related issue to CVE-2012-2660 and CVE-2012-2694.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399170
8235	CVE-2012-6712			In the Linux kernel before 3.4, a buffer overflow occurs in drivers/net/wireless/iwlwifi/iwl-agn-sta.c, which will cause at least memory corruption.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4548
8236	CVE-2012-6711	Medium	HIGH	A heap-based buffer overflow exists in GNU Bash before 4.3 when wide characters, not supported by the current locale set in the LC_CTYPE environment variable, are printed through the echo built-in function. A local attacker, who can provide data to print through the echo -e built-in function, may use this flaw to crash a script or execute code with the privileges of the bash process. This occurs because ansicstr() in lib/sh/strtrans.c mishandles u32cconv().	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4300
8237	CVE-2012-6704	HIGH	High	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 3.5 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUF or (2) SO_RCVBUF option.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-2861
8238	CVE-2012-6703	High		Integer overflow in the snd_compr_allocate_buffer function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.6-rc6-next-20120917 allows local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call.CWE-190: Integer Overflow or Wraparound	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-1115
8239	CVE-2012-6702	Medium		Expat, when used in a parser that has not called XML_SetHashSalt or passed it a seed of 0, makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms via vectors involving use of the srand function.	expat	Unchanged	8.0.0.8	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-931
8240	CVE-2012-6701	High		Integer overflow in fs/aio.c in the Linux kernel before 3.4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec.CWE-190: Integer Overflow or Wraparound	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-643
8241	CVE-2012-6689	High		The netlink_sendmsg function in net/netlink/af_netlink.c in the Linux kernel before 3.5.5 does not validate the dst_pid field, which allows local users to have an unspecified impact by spoofing Netlink messages.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-565
8242	CVE-2012-6657	Medium		The sock_setsockopt function in net/core/sock.c in the Linux kernel before 3.5.7 does not ensure that a keepalive action is associated with a stream socket, which allows local users to cause a denial of service (system crash) by leveraging the ability to create a raw socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8560
8243	CVE-2012-6656	Medium		iconvdata/ibm930.c in GNU C Library (aka glibc) before 2.16 allows context-dependent attackers to cause a denial of service (out-of-bounds read) via a multibyte character value of 0xffff to the iconv function when converting IBM930 encoded data to UTF-8.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2413
8244	CVE-2012-6647	Medium		The futex_wait_requeue_pi function in kernel/futex.c in the Linux kernel before 3.5.1 does not ensure that calls have two different futex addresses, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted FUTEX_WAIT_REQUEUE_PI command.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7578
8245	CVE-2012-6638	High		The tcp_rcv_state_process function in net/ipv4/tcp_input.c in the Linux kernel before 3.2.24 allows remote attackers to cause a denial of service (kernel resource consumption) via a flood of SYN+FIN TCP packets, a different vulnerability than CVE-2012-2663.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6854
8246	CVE-2012-6618	Low		The av_probe_input_buffer function in libavformat/utils.c in FFmpeg before 1.0.2, when running with certain -probesize values, allows remote attackers to cause a denial of service (crash) via a crafted MP3 file, possibly related to frame size or lack of sufficient frames to estimate rate.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2506
8247	CVE-2012-6617	Medium		The prepare_sdp_description function in ffserver.c in FFmpeg before 1.0.2 allows remote attackers to cause a denial of service (crash) via vectors related to the rtp format.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2511
8248	CVE-2012-6616	Medium		The mov_text_decode_frame function in libavcodec/movtextdec.c in FFmpeg before 1.0.2 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via crafted 3GPP TS 26.245 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2517
8249	CVE-2012-6615	Medium		The ff_ass_split_override_codes function in libavcodec/ass_split.c in FFmpeg before 1.0.2 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a subtitle dialog without text.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference AC:M for notation of file in bug report ffmpeg crashes reproducibly when converting files with some subtitles. i've seen the crash with self-compiled ffmpeg 1.0 as well as the Mac OS X binary (linked to from the hompage) for 1.0.1. download the sample file:https://dl.dropbox.com/u/7221986/ffmpeg-bug.mkv	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2521

	A	B	C	D	E	F	G	H	I	J	K	L	M
8250	CVE-2012-6612	High		The (1) UpdateRequestHandler for XSLT or (2) XPathEntityProcessor in Apache Solr before 4.1 allows remote attackers to have an unspecified impact via XML data containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, different vectors than CVE-2013-6407.	apache solr	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448759
8251	CVE-2012-6607	Low		The transform_save function in transform_save in Augeas before 1.0.0 allows local users to overwrite arbitrary files and obtain sensitive information via a symlink attack on a .augsave file in a backup save action, a different vector than CVE-2012-0786.	augeas	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445839
8252	CVE-2012-6552	High		Unspecified vulnerability in admin/action.php in phpVMS 2.1.x before 2.1.935 has unknown impact and attack vectors.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00419901
8253	CVE-2012-6551	Medium		The default configuration of Apache ActiveMQ before 5.8.0 enables a sample web application, which allows remote attackers to cause a denial of service (broker resource consumption) via HTTP requests.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415975
8254	CVE-2012-6549	Low		The isofs_export_encode_fh function in fs/isofs/export.c in the Linux kernel before 3.6 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel heap memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413568
8255	CVE-2012-6548	Low		The udf_encode_fh function in fs/udf/namei.c in the Linux kernel before 3.6 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel heap memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413588
8256	CVE-2012-6547	Low		The __tun_chr_ioctl function in drivers/net/tun.c in the Linux kernel before 3.6 does not initialize a certain structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413578
8257	CVE-2012-6546	Low		The ATM implementation in the Linux kernel before 3.6 does not initialize certain structures, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413559
8258	CVE-2012-6545	Low		The Bluetooth RFCOMM implementation in the Linux kernel before 3.6 does not properly initialize certain structures, which allows local users to obtain sensitive information from kernel memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413549
8259	CVE-2012-6544	Low		The Bluetooth protocol stack in the Linux kernel before 3.6 does not properly initialize certain structures, which allows local users to obtain sensitive information from kernel stack memory via a crafted application that targets the (1) L2CAP or (2) HCI implementation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413571
8260	CVE-2012-6543	Low		The l2tp_ip6_getname function in net/l2tp/l2tp_ip6.c in the Linux kernel before 3.6 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413558
8261	CVE-2012-6542	Low		The llc_ui_getname function in net/llc/af_llc.c in the Linux kernel before 3.6 has an incorrect return value in certain circumstances, which allows local users to obtain sensitive information from kernel stack memory via a crafted application that leverages an uninitialized pointer argument.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413566
8262	CVE-2012-6541	Low		The ccid3_hc_tx_getsockopt function in net/dccp/ccids/ccid3.c in the Linux kernel before 3.6 does not initialize a certain structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413553
8263	CVE-2012-6540	Low		The do_ip_vs_get_ctl function in net/netfilter/ipvs/ip_vs_ctl.c in the Linux kernel before 3.6 does not initialize a certain structure for IP_VS_SO_GET_TIMEOUT commands, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413580
8264	CVE-2012-6539	Low		The dev_ifconf function in net/socket.c in the Linux kernel before 3.6 does not initialize a certain structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413572
8265	CVE-2012-6538	Low		The copy_to_user_auth function in net/xfrm/xfrm_user.c in the Linux kernel before 3.6 uses an incorrect C library function for copying a string, which allows local users to obtain sensitive information from kernel heap memory by leveraging the CAP_NET_ADMIN capability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413579
8266	CVE-2012-6537	Low		net/xfrm/xfrm_user.c in the Linux kernel before 3.6 does not initialize certain structures, which allows local users to obtain sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413589
8267	CVE-2012-6536	Low		net/xfrm/xfrm_user.c in the Linux kernel before 3.6 does not verify that the actual Netlink message length is consistent with a certain header field, which allows local users to obtain sensitive information from kernel heap memory by leveraging the CAP_NET_ADMIN capability and providing a (1) new or (2) updated state.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413564
8268	CVE-2012-6525	High		SQL injection vulnerability in members.php in PHPBridges allows remote attackers to execute arbitrary SQL commands via the id parameter.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402348
8269	CVE-2012-6516	High		SQL injection vulnerability in PHP Ticket System Beta 1 allows remote attackers to execute arbitrary SQL commands via the q parameter to index.php.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402345
8270	CVE-2012-6505	Medium		Cross-site scripting (XSS) vulnerability in mods/hours/data/get_hours.php in PHP Volunteer Management 1.0.2 allows remote attackers to inject arbitrary web script or HTML via the id parameter.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402368

	A	B	C	D	E	F	G	H	I	J	K	L	M
8271	CVE-2012-6504	High		SQL injection vulnerability in mods/hours/data/get_hours.php in PHP Volunteer Management 1.0.2 allows remote attackers to execute arbitrary SQL commands via the id parameter.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402371
8272	CVE-2012-6497	Medium		The Authlogic gem for Ruby on Rails, when used with certain versions before 3.2.10, makes potentially unsafe find_by_id method calls, which might allow remote attackers to conduct CVE-2012-6496 SQL injection attacks via a crafted parameter in environments that have a known secret_token value, as demonstrated by a value contained in secret_token.rb in an open-source product.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399168
8273	CVE-2012-6496	High		SQL injection vulnerability in the Active Record component in Ruby on Rails before 3.0.18, 3.1.x before 3.1.9, and 3.2.x before 3.2.10 allows remote attackers to execute arbitrary SQL commands via a crafted request that leverages incorrect behavior of dynamic finders in applications that can use unexpected data types in certain find_by_ method calls.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399173
8274	CVE-2012-6329	High		The _compile function in Maketext.pm in the Locale::Maketext implementation in Perl before 5.17.7 does not properly handle backslashes and fully qualified method names during compilation of bracket notation, which allows context-dependent attackers to execute arbitrary commands via crafted input to an application that accepts translation strings from users, as demonstrated by the TWiki application before 5.1.3, and the Foswiki application 1.0.x through 1.0.10 and 1.1.x through 1.1.6.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399175
8275	CVE-2012-6151	Medium		Net-SNMP 5.7.1 and earlier, when AgentX is registering to handle a MIB and processing GETNEXT requests, allows remote attackers to cause a denial of service (crash or infinite loop, CPU consumption, and hang) by causing the AgentX subagent to timeout.	Net-snmp	Unchanged	8.0.0.26	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6724
8276	CVE-2012-6150	Low		The winbind_name_list_to_sid_string_list function in nsswitch/pam_winbind.c in Samba through 4.1.2 handles invalid require_membership_of group names by accepting authentication by any user, which allows remote authenticated users to bypass intended access restrictions in opportunistic circumstances by leveraging an administrator's pam_winbind configuration-file mistake.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448723
8277	CVE-2012-6139	Medium		libxslt before 1.1.28 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via an (1) empty match attribute in a XSL key to the xsltAddKey function in keys.c or (2) uninitialized variable to the xsltDocumentFunction function in functions.c.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	libxslt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415973
8278	CVE-2012-6113	Medium		The openssl_encrypt function in ext/openssl/openssl.c in PHP 5.3.9 through 5.3.13 does not initialize a certain variable, which allows remote attackers to obtain sensitive information from process memory by providing zero bytes of input data.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402361
8279	CVE-2012-6112	Medium		classes/GoogleSpell.php in the PHP Spellchecker (aka Google Spellchecker) addon before 2.0.6.1 for TinyMCE, as used in Moodle 2.1.x before 2.1.10, 2.2.x before 2.2.7, 2.3.x before 2.3.4, and 2.4.x before 2.4.1 and other products, does not properly handle control characters, which allows remote attackers to trigger arbitrary outbound HTTP requests via a crafted string.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402373
8280	CVE-2012-6097	Medium		File descriptor leak in cronie 1.4.8, when running in certain environments, might allow local users to read restricted files, as demonstrated by reading /etc/crontab.	cronie	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413592
8281	CVE-2012-6093	Medium		The QSslSocket::sslErrors function in Qt before 4.6.5, 4.7.x before 4.7.6, 4.8.x before 4.8.5, when using certain versions of openSSL, uses an incompatible structure layout that can read memory from the wrong location, which causes Qt to report an incorrect error when certificate validation fails and might cause users to make unsafe security decisions to accept a certificate.	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406213
8282	CVE-2012-6092	Medium		Multiple cross-site scripting (XSS) vulnerabilities in the web demos in Apache ActiveMQ before 5.8.0 allow remote attackers to inject arbitrary web script or HTML via (1) the refresh parameter to PortfolioPublishServlet.java (aka demo/portfolioPublish or Market Data Publisher), or vectors involving (2) debug logs or (3) subscribe messages in webapp/websocket/chat.js. NOTE: AMQ-4124 is covered by CVE-2012-6551.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415936
8283	CVE-2012-6088	Medium		The rpmpkgRead function in lib/package.c in RPM 4.10.x before 4.10.2 does not return an error code in certain situations involving an unparseable signature, which allows remote attackers to bypass RPM signature checks via a crafted package.	rpm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402372
8284	CVE-2012-6085	Medium		The read_block function in g10/import.c in GnuPG 1.4.x before 1.4.13 and 2.0.x through 2.0.19, when importing a key, allows remote attackers to corrupt the public keyring database or cause a denial of service (application crash) via a crafted length field of an OpenPGP packet.	gnupg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402349
8285	CVE-2012-6075	High		Buffer overflow in the e1000_receive function in the e1000 device driver (hw/e1000.c) in QEMU 1.3.0-rc2 and other versions, when the SBP and LPE flags are disabled, allows remote attackers to cause a denial of service (guest OS crash) and possibly execute arbitrary guest code via a large packet.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404143

	A	B	C	D	E	F	G	H	I	J	K	L	M
8286	CVE-2012-6063	High		Double free vulnerability in the sftp_mkdir function in sftp.c in libssh before 0.5.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors, a different vector than CVE-2012-4559.	libssh2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394607
8287	CVE-2012-6046	High		Static code injection vulnerability in admin/banners.php in PHP Enter allows remote attackers to inject arbitrary PHP code into horad.php via the code parameter.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392012
8288	CVE-2012-6043	Medium		Cross-site scripting (XSS) vulnerability in downloads.php in PHP-Fusion 7.02.04 allows remote attackers to inject arbitrary web script or HTML via the cat_id parameter.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392010
8289	CVE-2012-5887	Medium		The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 does not properly check for stale nonce values in conjunction with enforcement of proper credentials, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392075
8290	CVE-2012-5886	Medium		The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 caches information about the authenticated user within the session state, which makes it easier for remote attackers to bypass authentication via vectors related to the session ID.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392079
8291	CVE-2012-5885	Medium		The replay-countermeasure functionality in the HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.36, 6.x before 6.0.36, and 7.x before 7.0.30 tracks cnonce (aka client nonce) values instead of nonce (aka server nonce) and nc (aka nonce-count) values, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, a different vulnerability than CVE-2011-1184.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392011
8292	CVE-2012-5786	Medium		The wsdl_first_https sample code in distribution/src/main/release/samples/wsdl_first_https/src/main/ in Apache CXF, possibly 2.6.0, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00389435
8293	CVE-2012-5785	Medium		Apache Axis2/Java 1.6.2 and earlier does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00389438
8294	CVE-2012-5689	High		ISC BIND 9.8.x through 9.8.4-P1 and 9.9.x through 9.9.2-P1, in certain configurations involving DNS64 with a Response Policy Zone that lacks an AAAA rewrite rule, allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for an AAAA record.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402374
8295	CVE-2012-5688	High		ISC BIND 9.8.x before 9.8.4-P1 and 9.9.x before 9.9.2-P1, when DNS64 is enabled, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394610
8296	CVE-2012-5670	Medium		The _bdf_parse_glyphs function in FreeType before 2.4.11 allows context-dependent attackers to cause a denial of service (out-of-bounds write and crash) via vectors related to BDF fonts and an ENCODING field with a negative value.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402376
8297	CVE-2012-5669	Medium		The _bdf_parse_glyphs function in FreeType before 2.4.11 allows context-dependent attackers to cause a denial of service (crash) via vectors related to BDF fonts and an incorrect calculation that triggers an out-of-bounds read.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402351
8298	CVE-2012-5668	Medium		FreeType before 2.4.11 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to BDF fonts and the improper handling of an allocation error in the bdf_free_font function.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402377
8299	CVE-2012-5667	Medium		Multiple integer overflows in GNU Grep before 2.11 might allow context-dependent attackers to execute arbitrary code via vectors involving a long input line that triggers a heap-based buffer overflow.	grep	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399177
8300	CVE-2012-5664	High		SQL injection vulnerability in the Authlogic gem for Ruby on Rails allows remote attackers to execute arbitrary SQL commands via a crafted parameter in conjunction with a secret_token value, related to certain behavior of find_by_id and other find_by_ methods.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397029
8301	CVE-2012-5627	Medium		Oracle MySQL and MariaDB 5.5.x before 5.5.29, 5.3.x before 5.3.12, and 5.2.x before 5.2.14 does not modify the salt during multiple executions of the change_user command within the same connection which makes it easier for remote authenticated users to conduct brute force password guessing attacks.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439193
8302	CVE-2012-5624	Medium		The XMLHttpRequest object in Qt before 4.8.4 enables http redirection to the file scheme, which allows man-in-the-middle attackers to force the read of arbitrary local files and possibly obtain sensitive information via a file: URL to a QML application.Per http://www.ubuntu.com/usn/USN-1723-1/	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406232
8303	CVE-2012-5616	Low		Apache CloudStack 4.0.0-incubating and Citrix CloudPlatform (formerly Citrix CloudStack) before 3.0.6 stores sensitive information in the log4j.conf log file, which allows local users to obtain (1) the SSH private key as recorded by the createSSHKeyPair API, (2) the password of an added host as recorded by the AddHost API, or the password of an added VM as recorded by the (3) DeployVM or (4) ResetPasswordForVM API.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402365

	A	B	C	D	E	F	G	H	I	J	K	L	M
8304	CVE-2012-5615	Medium		MySQL 5.5.19 and possibly other versions, and MariaDB 5.5.28a, 5.3.11, 5.2.13, 5.1.66, and possibly other versions, generates different error messages with different time delays depending on whether a user name exists, which allows remote attackers to enumerate valid usernames.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394616
8305	CVE-2012-5614	Medium		MySQL 5.5.19 and possibly other versions, and MariaDB 5.5.28a and possibly other versions, allows remote authenticated users to cause a denial of service (mysqld crash) via a SELECT command with an UpdateXML command containing XML with a large number of unique, nested elements.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394608
8306	CVE-2012-5613	Medium		** DISPUTED ** MySQL 5.5.19 and possibly other versions, and MariaDB 5.5.28a and possibly other versions, when configured to assign the FILE privilege to users who should not have administrative privileges, allows remote authenticated users to gain privileges by leveraging the FILE privilege to create files as the MySQL administrator. NOTE: the vendor disputes this issue, stating that this is only a vulnerability when the administrator does not follow recommendations in the product's installation documentation. NOTE: it could be argued that this should not be included in CVE because it is a configuration issue.Per http://www.openwall.com/lists/oss-security/2012/12/02/3, this vulnerability is for linux-based software installations.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394613
8307	CVE-2012-5612	Medium		Heap-based buffer overflow in MySQL 5.5.19 and possibly other versions, and MariaDB 5.5.28a and possibly other versions, allows remote authenticated users to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code, as demonstrated using certain variations of the (1) USE, (2) SHOW TABLES, (3) DESCRIBE, (4) SHOW FIELDS FROM, (5) SHOW COLUMNS FROM, (6) SHOW INDEX FROM, (7) CREATE TABLE, (8) DROP TABLE, (9) ALTER TABLE, (10) DELETE FROM, (11) UPDATE, and (12) SET PASSWORD commands.Per http://www.openwall.com/lists/oss-security/2012/12/02/3, this vulnerability is for linux-based software installations.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394619
8308	CVE-2012-5611	Medium		Stack-based buffer overflow in MySQL 5.5.19, 5.1.53, and possibly other versions, and MariaDB 5.5.2.x before 5.5.28a, 5.3.x before 5.3.11, 5.2.x before 5.2.13 and 5.1.x before 5.1.66, allows remote authenticated users to execute arbitrary code via a long argument to the GRANT FILE command.per http://www.openwall.com/lists/oss-security/2012/12/02/3, this vulnerability is only on linux-based software installations	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394611
8309	CVE-2012-5581	Medium		Stack-based buffer overflow in tif_dir.c in LibTIFF before 4.0.2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted DOTRANGE tag in a TIFF image.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399178
8310	CVE-2012-5580	High		Format string vulnerability in the print_proxies function in bin/proxy.c in libproxy 0.3.1 might allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via format string specifiers in a proxy name, as demonstrated using the http_proxy environment variable or a PAC file.	libproxy	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8668
8311	CVE-2012-5577	MEDIUM	HIGH	Python keyring lib before 0.10 created keyring files with world-readable permissions.	python-keyring	Unchanged	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5184
8312	CVE-2012-5575	Medium		Apache CFX 2.5.x before 2.5.10, 2.6.x before CXF 2.6.7, and 2.7.x before CXF 2.7.4 does not verify that a specified cryptographic algorithm is allowed by the WS-SecurityPolicy AlgorithmSuite definition before decrypting, which allows remote attackers to force CXF to use weaker cryptographic algorithms than intended and makes it easier to decrypt communications, aka XML Encryption backwards compatibility attack.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00433023
8313	CVE-2012-5568	Medium		Apache Tomcat through 7.0.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394612
8314	CVE-2012-5533	Medium		The http_request_split_value function in request.c in lighttpd 1.4.32 allows remote attackers to cause a denial of service (infinite loop) via a request with a header containing an empty token, as demonstrated using the Connection: TE,,Keep-Alive header.	lighttpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392071
8315	CVE-2012-5532	Medium		The main function in tools/hv/hv_kvp_daemon.c in hypervkvpd, as distributed in the Linux kernel before 3.8-rc1, allows local users to cause a denial of service (daemon exit) via a crafted application that sends a Netlink message. NOTE: this vulnerability exists because of an incorrect fix for CVE-2012-2669.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397030
8316	CVE-2012-5519	High		CUPS 1.4.4, when running in certain Linux distributions such as Debian GNU/Linux, stores the web interface administrator key in /var/run/cups/certs/0 using certain permissions, which allows local users in the lpadmin group to read or write arbitrary files as root by leveraging the web interface.	cups	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392016
8317	CVE-2012-5517	Medium		The online_pages function in mm/memory_hotplug.c in the Linux kernel before 3.6 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact in opportunistic circumstances by using memory that was hot-added by an administrator.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397021
8318	CVE-2012-5469	High		The Portable phpMyAdmin plugin before 1.3.1 for WordPress allows remote attackers to bypass authentication and obtain phpMyAdmin console access via a direct request to wp-content/plugins/portable-phpmyadmin/wp-pma-mod.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397028

	A	B	C	D	E	F	G	H	I	J	K	L	M
8319	CVE-2012-5383	Medium		** DISPUTED ** Untrusted search path vulnerability in the installation functionality in Oracle MySQL 5.5.28, when installed in the top-level C:\ directory, might allow local users to gain privileges via a Trojan horse DLL in the C:\MySQL\MySQL Server 5.5\bin directory, which may be added to the PATH system environment variable by an administrator, as demonstrated by a Trojan horse wlbsctrl.dll file used by the IKE and AuthIP IPsec Keying Modules system service in Windows Vista SP1, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 Release Preview. NOTE: CVE disputes this issue because the unsafe PATH is established only by a separate administrative action that is not a default part of the MySQL installation.Per: http://cwe.mitre.org/data/definitions/426.html 'CWE-426 Untrusted Search Path'	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382758
8320	CVE-2012-5381	Medium		** DISPUTED ** Untrusted search path vulnerability in the installation functionality in PHP 5.3.17, when installed in the top-level C:\ directory, might allow local users to gain privileges via a Trojan horse DLL in the C:\PHP directory, which may be added to the PATH system environment variable by an administrator, as demonstrated by a Trojan horse wlbsctrl.dll file used by the IKE and AuthIP IPsec Keying Modules system service in Windows Vista SP1, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 Release Preview. NOTE: CVE disputes this issue because the unsafe PATH is established only by a separate administrative action that is not a default part of the PHP installation.Per: http://cwe.mitre.org/data/definitions/426.html 'CWE-426 Untrusted Search Path'	php.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382744
8321	CVE-2012-5380	Medium		** DISPUTED ** Untrusted search path vulnerability in the installation functionality in Ruby 1.9.3-p194, when installed in the top-level C:\ directory, might allow local users to gain privileges via a Trojan horse DLL in the C:\Ruby193\bin directory, which may be added to the PATH system environment variable by an administrator, as demonstrated by a Trojan horse wlbsctrl.dll file used by the IKE and AuthIP IPsec Keying Modules system service in Windows Vista SP1, Windows Server 2008 SP2, Windows 7 SP1, and Windows 8 Release Preview. NOTE: CVE disputes this issue because the unsafe PATH is established only by a separate administrative action that is not a default part of the Ruby installation.Per: http://cwe.mitre.org/data/definitions/426.html 'CWE-426 Untrusted Search Path'	ruby.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382753
8322	CVE-2012-5375	Medium		The CRC32C feature in the Btrfs implementation in the Linux kernel before 3.8-rc1 allows local users to cause a denial of service (prevention of file creation) by leveraging the ability to write to a directory important to the victim, and creating a file with a crafted name that is associated with a specific CRC32C hash value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406223
8323	CVE-2012-5374	Medium		The CRC32C feature in the Btrfs implementation in the Linux kernel before 3.8-rc1 allows local users to cause a denial of service (extended runtime of kernel code) by creating many different files whose names are associated with the same CRC32C hash value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406223
8324	CVE-2012-5371	Medium		Ruby (aka CRuby) 1.9 before 1.9.3-p327 and 2.0 before r37575 computes hash values without properly restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table, as demonstrated by a universal multicollision attack against a variant of the MurmurHash2 algorithm, a different vulnerability than CVE-2011-4815.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392074
8325	CVE-2012-5370	Medium		JRuby computes hash values without properly restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table, as demonstrated by a universal multicollision attack against the MurmurHash2 algorithm, a different vulnerability than CVE-2011-4838.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392006
8326	CVE-2012-5368	Medium		phpMyAdmin 3.5.x before 3.5.3 uses JavaScript code that is obtained through an HTTP session to phpmyadmin.net without SSL, which allows man-in-the-middle attackers to conduct cross-site scripting (XSS) attacks by modifying this code.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386307
8327	CVE-2012-5361	Medium		Libavcodec in FFmpeg before 0.11 allows remote attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3791
8328	CVE-2012-5360	High	High	Libavcodec in FFmpeg before 0.11 allows remote attackers to execute arbitrary code via a crafted QT file.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3366
8329	CVE-2012-5359	High	High	Libavcodec in FFmpeg before 0.11 allows remote attackers to execute arbitrary code via a crafted ASF file.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-3364
8330	CVE-2012-5351	Medium		Apache Axis2 allows remote attackers to forge messages and bypass authentication via a SAML assertion that lacks a Signature element, aka a Signature exclusion attack, a different vulnerability than CVE-2012-4418.	apache axis2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382759
8331	CVE-2012-5339	Low		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 3.5.x before 3.5.3 allow remote authenticated users to inject arbitrary web script or HTML via a crafted name of (1) an event, (2) a procedure, or (3) a trigger.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386319

	A	B	C	D	E	F	G	H	I	J	K	L	M
8332	CVE-2012-5195	High		Heap-based buffer overflow in the Perl_repeatcpy function in util.c in Perl 5.12.x before 5.12.5, 5.14.x before 5.14.3, and 5.15.x before 15.15.5 allows context-dependent attackers to cause a denial of service (memory consumption and crash) or possibly execute arbitrary code via the 'x' string repeat operator.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397023
8333	CVE-2012-5166	High		ISC BIND 9.x before 9.7.6-P4, 9.8.x before 9.8.3-P4, 9.9.x before 9.9.1-P4, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P4 allows remote attackers to cause a denial of service (named daemon hang) via unspecified combinations of resource records.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382754
8334	CVE-2012-5159	High		phpMyAdmin 3.5.2.2, as distributed by the cdnetworks-kr-1 mirror during an unspecified time frame in 2012, contains an externally introduced modification (Trojan Horse) in server_sync.php, which allows remote attackers to execute arbitrary PHP code via an eval injection attack.Although not found in all distributions of this software, the vulnerability was scored assuming that it was. End-users will need to identify whether their distribution does in fact contain the vulnerability.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382748
8335	CVE-2012-5134	Medium		Heap-based buffer underflow in the xmlParseAttValueComplex function in parser.c in libxml2 2.9.0 and earlier, as used in Google Chrome before 23.0.1271.91, allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted entities in an XML document.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392072
8336	CVE-2012-5096	Low		Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users with Server Privileges to affect availability via unknown vectors.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402367
8337	CVE-2012-5060	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.65 and earlier and 5.5.27 and earlier allows remote authenticated users to affect availability, related to GIS Extension.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402347
8338	CVE-2012-4579	Low		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 3.5.x before 3.5.2.2 allow remote authenticated users to inject arbitrary web script or HTML via a Table Operations (1) TRUNCATE or (2) DROP link for a crafted table name, (3) the Add Trigger popup within a Triggers page that references crafted table names, (4) an invalid trigger-creation attempt for a crafted table name, (5) crafted data in a table, or (6) a crafted tooltip label name during GIS data visualization, a different issue than CVE-2012-4345.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374004
8339	CVE-2012-4571	Low		Python Keyring 0.9.1 does not securely initialize the cipher when encrypting passwords for CryptedFileKeyring files, which makes it easier for local users to obtain passwords via a brute-force attack.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394614
8340	CVE-2012-4566	Medium		The DTLS support in radsecproxy before 1.6.2 does not properly verify certificates when there are configuration blocks with CA settings that are unrelated to the block being used for verifying the certificate chain, which might allow remote attackers to bypass intended access restrictions and spoof clients, a different vulnerability than CVE-2012-4523.	proxy	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392014
8341	CVE-2012-4565	Medium		The tcp_illinois_info function in net/ipv4/tcp_illinois.c in the Linux kernel before 3.4.19, when the net.ipv4.tcp_congestion_control illinois setting is enabled, allows local users to cause a denial of service (divide-by-zero error and OOPS) by reading TCP stats.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397020
8342	CVE-2012-4564	Medium		ppm2tiff does not check the return value of the TIFFScanlineSize function, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PPM image that triggers an integer overflow, a zero-memory allocation, and a heap-based buffer overflow.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00389437
8343	CVE-2012-4562	High		Multiple integer overflows in libssh before 0.5.3 allow remote attackers to cause a denial of service (infinite loop or crash) and possibly execute arbitrary code via unspecified vectors, which triggers a buffer overflow, infinite loop, or possibly some other unspecified vulnerabilities.	libssh2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394615
8344	CVE-2012-4561	Medium		The (1) publickey_make_dss, (2) publickey_make_rsa, (3) signature_from_string, (4) ssh_do_sign, and (5) ssh_sign_session_id functions in keys.c in libssh before 0.5.3 free an invalid pointer on an error path, which might allow remote attackers cause a denial of service (crash) via unspecified vectors.	libssh2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394618
8345	CVE-2012-4560	High		Multiple buffer overflows in libssh before 0.5.3 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via unspecified vectors.	libssh2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394609
8346	CVE-2012-4559	Medium		Multiple double free vulnerabilities in the (1) agent_sign_data function in agent.c, (2) channel_request function in channels.c, (3) ssh_userauth_pubkey function in auth.c, (4) sftp_parse_attr_3 function in sftp.c, and (5) try_publickey_from_file function in keyfiles.c in libssh before 0.5.3 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors.	libssh2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394617
8347	CVE-2012-4558	Medium		Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406226
8348	CVE-2012-4557	Medium		The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of service (worker consumption) via an expensive request.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00394606

	A	B	C	D	E	F	G	H	I	J	K	L	M
8349	CVE-2012-4542	Medium		block/scsi_ioctl.c in the Linux kernel through 3.8 does not properly consider the SCSI device class during authorization of SCSI commands, which allows local users to bypass intended access restrictions via an SG_IO ioctl call that leverages overlapping opcodes.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406231
8350	CVE-2012-4534	Low		org/apache/tomcat/util/net/NioEndpoint.java in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.28, when the NIO connector is used in conjunction with sendfile and HTTPS, allows remote attackers to cause a denial of service (infinite loop) by terminating the connection during the reading of a response.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397024
8351	CVE-2012-4530	Low		The load_script function in fs/binfmt_script.c in the Linux kernel before 3.7.2 does not properly handle recursion, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406222
8352	CVE-2012-4528	Medium		The mod_security2 module before 2.7.0 for the Apache HTTP Server allows remote attackers to bypass rules, and deliver arbitrary POST data to a PHP application, via a multipart request in which an invalid part precedes the crafted data.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397026
8353	CVE-2012-4523	Medium		radsecproxy before 1.6.1 does not properly verify certificates when there are configuration blocks with CA settings that are unrelated to the block being used for verifying the certificate chain, which might allow remote attackers to bypass intended access restrictions and spoof clients.	proxy	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392073
8354	CVE-2012-4522	Medium		The rb_get_path_check function in file.c in Ruby 1.9.3 before patchlevel 286 and Ruby 2.0.0 before r37163 allows context-dependent attackers to create files in unexpected locations or with unexpected names via a NUL byte in a file path.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392007
8355	CVE-2012-4508	Low		Race condition in fs/ext4/extents.c in the Linux kernel before 3.4.16 allows local users to obtain sensitive information from a deleted file by reading an extent that was not properly marked as uninitialized.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397018
8356	CVE-2012-4505	High		Heap-based buffer overflow in the px_pac_reload function in lib/pac.c in libproxy 0.2.x and 0.3.x allows remote servers to have an unspecified impact via a crafted Content-Length size in an HTTP response header for a proxy.pac file request, a different vulnerability than CVE-2012-4504.	libproxy	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00389434
8357	CVE-2012-4504	High		Stack-based buffer overflow in the url::get_pac function in url.cpp in libproxy 0.4.x before 0.4.9 allows remote servers to have an unspecified impact via a large proxy.pac file.	libproxy	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00389436
8358	CVE-2012-4481	Medium		The safe-level feature in Ruby 1.8.7 allows context-dependent attackers to modify strings via the NameError#to_s method when operating on Ruby objects. NOTE: this issue is due to an incomplete fix for CVE-2011-1005.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417551
8359	CVE-2012-4467	Medium		The (1) do_siocgstamp and (2) do_siocgstampns functions in net/socket.c in the Linux kernel before 3.5.4 use an incorrect argument order, which allows local users to obtain sensitive information from kernel memory or cause a denial of service (system crash) via a crafted ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382747
8360	CVE-2012-4466	Medium		Ruby 1.8.7 before patchlevel 371, 1.9.3 before patchlevel 286, and 2.0 before revision r37068 allows context-dependent attackers to bypass safe-level restrictions and modify untainted strings via the name_err_mesg_to_str API function, which marks the string as tainted, a different vulnerability than CVE-2011-1005.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415962
8361	CVE-2012-4464	Medium		Ruby 1.9.3 before patchlevel 286 and 2.0 before revision r37068 allows context-dependent attackers to bypass safe-level restrictions and modify untainted strings via the (1) exc_to_s or (2) name_err_to_s API function, which marks the string as tainted, a different vulnerability than CVE-2012-4466. NOTE: this issue might exist because of a CVE-2011-1005 regression.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00415934
8362	CVE-2012-4463	Medium		Midnight Commander (mc) 4.8.5 does not properly handle the (1) MC_EXT_SELECTED or (2) MC_EXT_ONLYTAGGED environment variables when multiple files are selected, which allows user-assisted remote attackers to execute arbitrary commands via a crafted file name.	midnight_commander.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382772
8363	CVE-2012-4461	Low		The KVM subsystem in the Linux kernel before 3.6.9, when running on hosts that use qemu userspace without XSAVE, allows local users to cause a denial of service (kernel OOPS) by using the KVM_SET_SREGS ioctl to set the X86_CR4_OSXSAVE bit in the guest cr4 register, then calling the KVM_RUN ioctl.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402343
8364	CVE-2012-4452	Low		MySQL 5.0.88, and possibly other versions and platforms, allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL data home directory, related to incorrect calculation of the mysql_unpacked_real_data_home value. NOTE: this vulnerability exists because of a CVE-2009-4030 regression, which was not omitted in other packages and versions such as MySQL 5.0.95 in Red Hat Enterprise Linux 6.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382750
8365	CVE-2012-4447	Medium		Heap-based buffer overflow in tif_pixarlog.c in LibTIFF before 4.0.3 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted TIFF image using the PixarLog Compression format.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386301

	A	B	C	D	E	F	G	H	I	J	K	L	M
8366	CVE-2012-4444	Medium		The ip6_frag_queue function in net/ipv6/reassembly.c in the Linux kernel before 2.6.36 allows remote attackers to bypass intended network restrictions via overlapping IPv6 fragments.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397019
8367	CVE-2012-4431	Medium		org/apache/catalina/filters/CsrfPreventionFilter.java in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.32 allows remote attackers to bypass the cross-site request forgery (CSRF) protection mechanism via a request that lacks a session identifier.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397031
8368	CVE-2012-4424	Medium		Stack-based buffer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string that triggers a malloc failure and use of the alloca function.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439181
8369	CVE-2012-4423	Medium		The virNetServerProgramDispatchCall function in libvirt before 0.10.2 allows remote attackers to cause a denial of service (NULL pointer dereference and segmentation fault) via an RPC call with (1) an event as the RPC number or (2) an RPC number whose value is in a gap in the RPC dispatch table.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392077
8370	CVE-2012-4418	Medium		Apache Axis2 allows remote attackers to forge messages and bypass authentication via an XML Signature wrapping attack.	apache axis2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382761
8371	CVE-2012-4414	Medium		Multiple SQL injection vulnerabilities in the replication code in Oracle MySQL possibly before 5.5.29, and MariaDB 5.1.x through 5.1.62, 5.2.x through 5.2.12, 5.3.x through 5.3.7, and 5.5.x through 5.5.25, allow remote authenticated users to execute arbitrary SQL commands via vectors related to the binary log. NOTE: as of 20130116, Oracle has not commented on claims from a downstream vendor that the fix in MySQL 5.5.29 is incomplete.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402360
8372	CVE-2012-4412	High		Integer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a heap-based buffer overflow.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00439214
8373	CVE-2012-4398	Medium		The __request_module function in kernel/kmod.c in the Linux kernel before 3.4 does not set a certain killable attribute, which allows local users to cause a denial of service (memory consumption) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406209
8374	CVE-2012-4388	Medium		The sapi_header_op function in main/SAPI.c in PHP 5.4.0RC2 through 5.4.0 does not properly determine a pointer during checks for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-1398.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376784
8375	CVE-2012-4387	Medium		Apache Struts 2.0.0 through 2.3.4 allows remote attackers to cause a denial of service (CPU consumption) via a long parameter name, which is processed as an OGNL expression.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376781
8376	CVE-2012-4386	Medium		The token check mechanism in Apache Struts 2.0.0 through 2.3.4 does not properly validate the token name configuration parameter, which allows remote attackers to perform cross-site request forgery (CSRF) attacks by setting the token name configuration parameter to a session attribute.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376788
8377	CVE-2012-4345	Low		Multiple cross-site scripting (XSS) vulnerabilities in the Database Structure page in phpMyAdmin 3.4.x before 3.4.11.1 and 3.5.x before 3.5.2.2 allow remote authenticated users to inject arbitrary web script or HTML via (1) a crafted table name during table creation, or a (2) Empty link or (3) Drop link for a crafted table name.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00373996
8378	CVE-2012-4247	Medium		Multiple cross-site scripting (XSS) vulnerabilities in lists/admin/index.php in phpList before 2.10.19 allow remote attackers to inject arbitrary web script or HTML via the (1) remote_user, (2) remote_database, (3) remote_userprefix, (4) remote_password, or (5) remote_prefix parameter to the import4 page; or the (6) id parameter to the bouncerule page.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370213
8379	CVE-2012-4246	Medium		Multiple cross-site scripting (XSS) vulnerabilities in lists/admin/index.php in phpList before 2.10.19 allow remote attackers to inject arbitrary web script or HTML via the (1) page parameter; or the (2) footer, (3) status, or (4) testtarget parameter in the send page.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370222
8380	CVE-2012-4244	High		ISC BIND 9.x before 9.7.6-P3, 9.8.x before 9.8.3-P3, 9.9.x before 9.9.1-P3, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P3 allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for a long resource record.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376774
8381	CVE-2012-4219	Medium		show_config_errors.php in phpMyAdmin 3.5.x before 3.5.2.1 allows remote attackers to obtain sensitive information via a direct request, which reveals the installation path in an error message, related to lack of inclusion of the common.inc.php library file.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374006
8382	CVE-2012-4025	Medium		Integer overflow in the queue_init function in unsquashfs.c in Squashfs 4.2 and earlier allows remote attackers to execute arbitrary code via a crafted block_log field in the superblock of a .sqsh file, leading to a heap-based buffer overflow.	squashfs	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366813

	A	B	C	D	E	F	G	H	I	J	K	L	M
8383	CVE-2012-4024	Medium		Stack-based buffer overflow in the get_component function in unsquashfs.c in unsquashfs in Squashfs 4.2 and earlier allows remote attackers to execute arbitrary code via a crafted list file (aka a crafted file for the -ef option). NOTE: probably in most cases, the list file is a trusted file constructed by the program's user; however, there are some realistic situations in which a list file would be obtained from an untrusted remote source.	squashfs	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366804
8384	CVE-2012-4001	Medium		The mod_pagespeed module before 0.10.22.6 for the Apache HTTP Server does not properly verify its host name, which allows remote attackers to trigger HTTP requests to arbitrary hosts via unspecified vectors, as demonstrated by requests to intranet servers.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382765
8385	CVE-2012-3955	High		ISC DHCP 4.1.x before 4.1-ESV-R7 and 4.2.x before 4.2.4-P2 allows remote attackers to cause a denial of service (daemon crash) in opportunistic circumstances by establishing an IPv6 lease in an environment where the lease expiration time is later reduced.	dhcp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376775
8386	CVE-2012-3954	Low		Multiple memory leaks in ISC DHCP 4.1.x and 4.2.x before 4.2.4-P1 and 4.1-ESV before 4.1-ESV-R6 allow remote attackers to cause a denial of service (memory consumption) by sending many requests.	dhcp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366782
8387	CVE-2012-3953	High		SQL injection vulnerability in admin/index.php in phpList before 2.10.19 allows remote administrators to execute arbitrary SQL commands via the delete parameter to the editattributes page.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370220
8388	CVE-2012-3952	Low		Cross-site scripting (XSS) vulnerability in admin/index.php in phpList before 2.10.19 allows remote attackers to inject arbitrary web script or HTML via the unconfirmed parameter to the user page.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370226
8389	CVE-2012-3868	Medium		Race condition in the ns_client structure management in ISC BIND 9.9.x before 9.9.1-P2 allows remote attackers to cause a denial of service (memory consumption or process exit) via a large volume of TCP queries.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366805
8390	CVE-2012-3846	Medium		Cross-site scripting (XSS) vulnerability in index.php in PHP-pastebin 2.1 allows remote attackers to inject arbitrary web script or HTML via the title parameter.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362913
8391	CVE-2012-3817	High		ISC BIND 9.4.x, 9.5.x, 9.6.x, and 9.7.x before 9.7.6-P2; 9.8.x before 9.8.3-P2; 9.9.x before 9.9.1-P2; and 9.6-ESV before 9.6-ESV-R7-P2, when DNSSEC validation is enabled, does not properly initialize the failing-query cache, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) by sending many queries.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366815
8392	CVE-2012-3588	Medium		Directory traversal vulnerability in preview.php in the Plugin Newsletter plugin 1.5 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the data parameter.	plugin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359358
8393	CVE-2012-3585	High		Heap-based buffer overflow in jpeg_ls.dll in the Jpeg_LS (aka JLS) plugin in the formats plugins in IrfanView PlugIns before 4.34 allows remote attackers to execute arbitrary code via a crafted JLS file.	plugins	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362919
8394	CVE-2012-3571	Medium		ISC DHCP 4.1.2 through 4.2.4 and 4.1-ESV before 4.1-ESV-R6 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a malformed client identifier.	dhcp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366779
8395	CVE-2012-3570	Medium		Buffer overflow in ISC DHCP 4.2.x before 4.2.4-P1, when DHCPv6 mode is enabled, allows remote attackers to cause a denial of service (segmentation fault and daemon exit) via a crafted client identifier parameter.	dhcp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366792
8396	CVE-2012-3552	Medium		The IP implementation in the Linux kernel before 3.0 might allow remote attackers to cause a denial of service (slab corruption and system crash) by sending packets to an application that sets socket options during the handling of network traffic.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382771
8397	CVE-2012-3547	Medium		Stack-based buffer overflow in the cbtls_verify function in FreeRADIUS 2.1.10 through 2.1.12, when using TLS-based EAP methods, allows remote attackers to cause a denial of service (server crash) and possibly execute arbitrary code via a long not after timestamp in a client certificate.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413557
8398	CVE-2012-3546	Medium		org/apache/catalina/realm/ RealmBase.java in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.30, when FORM authentication is used, allows remote attackers to bypass security-constraint checks by leveraging a previous setUserPrincipal call and then placing /j_security_check at the end of a URI.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397016
8399	CVE-2012-3544	Medium		Apache Tomcat 6.x before 6.0.37 and 7.x before 7.0.30 does not properly handle chunk extensions in chunked transfer coding, which allows remote attackers to cause a denial of service by streaming data.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421906
8400	CVE-2012-3520	Low		The Netlink implementation in the Linux kernel before 3.2.30 does not properly handle messages that lack SCM_CREDENTIALS data, which might allow local users to spoof Netlink communication via a crafted message, as demonstrated by a message to (1) Avahi or (2) NetworkManager.	linux.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382749
8401	CVE-2012-3515	High		Qemu, as used in Xen 4.0, 4.1 and possibly other products, when emulating certain devices with a virtual console backend, allows local OS guest users to gain privileges via a crafted escape VT100 sequence that triggers the overwrite of a device model's address space.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392008
8402	CVE-2012-3511	Medium		Multiple race conditions in the madvise_remove function in mm/madvise.c in the Linux kernel before 3.4.5 allow local users to cause a denial of service (use-after-free and system crash) via vectors involving a (1) munmap or (2) close system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382768

	A	B	C	D	E	F	G	H	I	J	K	L	M
8403	CVE-2012-3510	Medium		Use-after-free vulnerability in the xacct_add_tsk function in kernel/tsacct.c in the Linux kernel before 2.6.19 allows local users to obtain potentially sensitive information from kernel memory or cause a denial of service (system crash) via a taskstats TASKSTATS_CMD_ATTR_PID command.	linux.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382751
8404	CVE-2012-3509	Medium		Multiple integer overflows in the (1) _objalloc_alloc function in objalloc.c and (2) objalloc_alloc macro in include/objalloc.h in GNU libiberty, as used by binutils 2.22, allow remote attackers to cause a denial of service (crash) via vectors related to the addition of CHUNK_HEADER_SIZE to the length, which triggers a heap-based buffer overflow.	gnu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376786
8405	CVE-2012-3506	High		Unspecified vulnerability in the Apache Open For Business Project (aka OFBiz) 10.04.x before 10.04.03 has unknown impact and attack vectors.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386315
8406	CVE-2012-3502	Medium		The proxy functionality in (1) mod_proxy_ajp.c in the mod_proxy_ajp module and (2) mod_proxy_http.c in the mod_proxy_http module in the Apache HTTP Server 2.4.x before 2.4.3 does not properly determine the situations that require closing a back-end connection, which allows remote attackers to obtain sensitive information in opportunistic circumstances by reading a response that was intended for a different client.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00373999
8407	CVE-2012-3499	Medium		Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00406211
8408	CVE-2012-3489	Medium		The xml_parse function in the libxml2 support in the core server component in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 allows remote authenticated users to determine the existence of arbitrary files or URLs, and possibly obtain file or URL content that triggers a parsing error, via an XML value that refers to (1) a DTD or (2) an entity, related to an XML External Entity (aka XXE) issue.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382770
8409	CVE-2012-3488	Medium		The libxslt support in contrib/xml2 in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 does not properly restrict access to files and URLs, which allows remote authenticated users to modify data, obtain sensitive information, or trigger outbound traffic to arbitrary external hosts by leveraging (1) stylesheet commands that are permitted by the libxslt security options or (2) an xslt_process feature, related to an XML External Entity (aka XXE) issue.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382763
8410	CVE-2012-3480	Medium		Multiple integer overflows in the (1) strtod, (2) strtof, (3) strtold, (4) strtod_l, and other unspecified related functions in stdlib in GNU C Library (aka glibc or libc6) 2.16 allow local users to cause a denial of service (application crash) and possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374005
8411	CVE-2012-3467	Medium		Apache QPID 0.14, 0.16, and earlier uses a NullAuthenticator mechanism to authenticate catch-up shadow connections to AMQP brokers, which allows remote attackers to bypass authentication.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374016
8412	CVE-2012-3466	Medium		GNOME gnome-keyring 3.4.0 through 3.4.1, when gpg-cache-method is set to idle or timeout, does not properly limit the amount of time a passphrase is cached, which allows attackers to have an unspecified impact via unknown attack vectors.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386302
8413	CVE-2012-3465	Medium		Cross-site scripting (XSS) vulnerability in actionpack/lib/action_view/helpers/sanitize_helper.rb in the strip_tags helper in Ruby on Rails before 3.0.17, 3.1.x before 3.1.8, and 3.2.x before 3.2.8 allows remote attackers to inject arbitrary web script or HTML via malformed HTML markup.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370225
8414	CVE-2012-3464	Medium		Cross-site scripting (XSS) vulnerability in activesupport/lib/active_support/core_ext/string/output_safety.rb in Ruby on Rails before 3.0.17, 3.1.x before 3.1.8, and 3.2.x before 3.2.8 might allow remote attackers to inject arbitrary web script or HTML via vectors involving a ' (quote) character.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370227
8415	CVE-2012-3463	Medium		Cross-site scripting (XSS) vulnerability in actionpack/lib/action_view/helpers/form_tag_helper.rb in Ruby on Rails 3.x before 3.0.17, 3.1.x before 3.1.8, and 3.2.x before 3.2.8 allows remote attackers to inject arbitrary web script or HTML via the prompt field to the select_tag helper.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370209
8416	CVE-2012-3452	Low		gnome-screensaver 3.4.x before 3.4.4 and 3.5.x before 3.5.4, when multiple screens are used, only locks the screen with the active focus, which allows physically proximate attackers to bypass screen locking and access an unattended workstation.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370215
8417	CVE-2012-3450	Low		pdo_sql_parser.re in the PDO extension in PHP before 5.3.14 and 5.4.x before 5.4.4 does not properly determine the end of the query string during parsing of prepared statements, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted parameter value.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370223
8418	CVE-2012-3446	Medium		Apache Libcloud before 0.11.1 uses an incorrect regular expression during verification of whether the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a crafted certificate.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00389433

	A	B	C	D	E	F	G	H	I	J	K	L	M
8419	CVE-2012-3445	Low		The virTypedParameterArrayClear function in libvirt 0.9.13 does not properly handle virDomain* API calls with typed parameters, which might allow remote authenticated users to cause a denial of service (libvirtd crash) via an RPC command with nparams set to zero, which triggers an out-of-bounds read or a free of an invalid pointer.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370216
8420	CVE-2012-3440	Medium		A certain Red Hat script for sudo 1.7.2 on Red Hat Enterprise Linux (RHEL) 5 allows local users to overwrite arbitrary files via a symlink attack on the /var/tmp/nsswitch.conf.bak temporary file.Additional information: https://rhn.redhat.com/errata/RHSA-2012-1149.html	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370218
8421	CVE-2012-3437	Medium		The Magick_png_malloc function in coders/png.c in ImageMagick 6.7.8-6 does not use the proper variable type for the allocation size, which might allow remote attackers to cause a denial of service (crash) via a crafted PNG file that triggers incorrect memory allocation.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370217
8422	CVE-2012-3430	Low		The rds_recvmsg function in net/rds/recv.c in the Linux kernel before 3.0.44 does not initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via a (1) recvfrom or (2) recvmsg system call on an RDS socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382762
8423	CVE-2012-3424	Medium		The decode_credentials method in actionpack/lib/action_controller/metal/http_authentication.rb in Ruby on Rails 3.x before 3.0.16, 3.1.x before 3.1.7, and 3.2.x before 3.2.7 converts Digest Authentication strings to symbols, which allows remote attackers to cause a denial of service by leveraging access to an application that uses a with_http_digest helper method, as demonstrated by the authenticate_or_request_with_http_digest method.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370224
8424	CVE-2012-3417	Medium		The good_client function in rquotad (rquota_svc.c) in Linux DiskQuota (aka quota) before 3.17 invokes the hosts_ctl function the first time without a host name, which might allow remote attackers to bypass TCP Wrappers rules in hosts.deny.	quota	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430961
8425	CVE-2012-3412	High		The sfc (aka Solarflare Solarstorm) driver in the Linux kernel before 3.2.30 allows remote attackers to cause a denial of service (DMA descriptor consumption and network-controller outage) via crafted TCP packets that trigger a small MSS value.	linux.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382752
8426	CVE-2012-3410	Medium		Stack-based buffer overflow in lib/sh/eaccess.c in GNU Bash before 4.2 patch 33 might allow local users to bypass intended restricted shell access via a long filename in /dev/fd, which is not properly handled when expanding the /dev/fd prefix.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374000
8427	CVE-2012-3406	Medium		The vfprintf function in stdio-common/vfprintf.c in GNU C Library (aka glibc) 2.5, 2.12, and probably other versions does not properly restrict the use of the alloca function when allocating the SPECS array, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (crash) or possibly execute arbitrary code via a crafted format string using positional parameters and a large number of format specifiers, a different vulnerability than CVE-2012-3404 and CVE-2012-3405.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6748
8428	CVE-2012-3405	Medium		The vfprintf function in stdio-common/vfprintf.c in libc in GNU C Library (aka glibc) 2.14 and other versions does not properly calculate a buffer length, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (segmentation fault and crash) via a format string with a large number of format specifiers that triggers desynchronization within the buffer size handling, a different vulnerability than CVE-2012-3404.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6738
8429	CVE-2012-3404	Medium		The vfprintf function in stdio-common/vfprintf.c in libc in GNU C Library (aka glibc) 2.12 and other versions does not properly calculate a buffer length, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (stack corruption and crash) via a format string that uses positional parameters and many format specifiers.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6766
8430	CVE-2012-3401	Medium		The t2p_read_tiff_init function in tiff2pdf (tools/tiff2pdf.c) in LibTIFF 4.0.2 and earlier does not properly initialize the T2P context struct pointer in certain error conditions, which allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted TIFF image that triggers a heap-based buffer overflow.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374012
8431	CVE-2012-3400	High		Heap-based buffer overflow in the udf_load_logicalvol function in fs/udf/super.c in the Linux kernel before 3.4.5 allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted UDF filesystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382760
8432	CVE-2012-3386	Medium		The make distcheck rule in GNU Automake before 1.11.6 and 1.12.x before 1.12.2 grants world-writable permissions to the extraction directory, which introduces a race condition that allows local users to execute arbitrary code via unspecified vectors.	automake	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370219
8433	CVE-2012-3378	Low		The register_application function in atk-adaptor/bridge.c in GNOME at-spi2-atk 2.5.2 does not seed the random number generator and generates predictable temporary file names, which makes it easier for local users to create or truncate files via a symlink attack on a temporary socket file in /tmp/at-spi2.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376789

	A	B	C	D	E	F	G	H	I	J	K	L	M
8434	CVE-2012-3376	High		DataNodes in Apache Hadoop 2.0.0 alpha does not check the BlockTokens of clients when Kerberos is enabled and the DataNode has checked out the same BlockPool twice from a NodeName, which might allow remote clients to read arbitrary blocks, write to blocks to which they only have read access, and have other unspecified impacts.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366786
8435	CVE-2012-3375	Medium		The epoll_ctl system call in fs/eventpoll.c in the Linux kernel before 3.2.24 does not properly handle ELOOP errors in EPOLL_CTL_ADD operations, which allows local users to cause a denial of service (file-descriptor consumption and system crash) via a crafted application that attempts to create a circular epoll dependency. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-1083.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382757
8436	CVE-2012-3365	Medium		The SQLite functionality in PHP before 5.3.15 allows remote attackers to bypass the open_basedir protection mechanism via unspecified vectors.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366796
8437	CVE-2012-3364	Medium		Multiple stack-based buffer overflows in the Near Field Communication Controller Interface (NCI) in the Linux kernel before 3.4.5 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via incoming frames with crafted length fields.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402356
8438	CVE-2012-3197	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.64 and earlier, and 5.5.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Replication.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386300
8439	CVE-2012-3180	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.65 and earlier, and 5.5.27 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386308
8440	CVE-2012-3177	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.65 and earlier, and 5.5.27 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386305
8441	CVE-2012-3173	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.63 and earlier, and 5.5.25 and earlier, allows remote authenticated users to affect availability via unknown vectors related to InnoDB Plugin.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386312
8442	CVE-2012-3167	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.63 and earlier, and 5.5.25 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Full Text Search.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386311
8443	CVE-2012-3166	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.63 and earlier, and 5.5.25 and earlier, allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386318
8444	CVE-2012-3163	High		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.64 and earlier, and 5.5.26 and earlier, allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Information Schema.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386296
8445	CVE-2012-3160	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.65 and earlier, and 5.5.27 and earlier, allows local users to affect confidentiality via unknown vectors related to Server Installation.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386314
8446	CVE-2012-3158	High		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.64 and earlier, and 5.5.26 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Protocol.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386317
8447	CVE-2012-3156	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386304
8448	CVE-2012-3150	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.64 and earlier, and 5.5.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386310
8449	CVE-2012-3149	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 and earlier allows remote authenticated users to affect confidentiality, related to MySQL Client.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386298
8450	CVE-2012-3147	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 and earlier allows remote attackers to affect integrity and availability, related to MySQL Client.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386309
8451	CVE-2012-3144	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386316
8452	CVE-2012-2925	High		SQL injection vulnerability in engine.php in Simple PHP Agenda 2.2.8 allows remote attackers to execute arbitrary SQL commands via the priority parameter in an addTodo action.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353073
8453	CVE-2012-2903	Medium		Multiple cross-site scripting (XSS) vulnerabilities in PHP Address Book 7.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) PATH_INFO to group.php, or the (2) target_language or (3) target_flag parameter to translate.php.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353044
8454	CVE-2012-2871	Medium		libxml2 2.9.0-rc1 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly support a cast of an unspecified variable during handling of XSL transforms, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document, related to the _xmlNs data structure in include/libxml/tree.h.Per: http://cwe.mitre.org/data/definitions/704.html 'CWE-704: Incorrect Type Conversion or Cast'	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376779

	A	B	C	D	E	F	G	H	I	J	K	L	M
8455	CVE-2012-2870	Medium		libxslt 1.1.26 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly manage memory, which might allow remote attackers to cause a denial of service (application crash) via a crafted XSLT expression that is not properly identified during XPath navigation, related to (1) the xsltCompileLocationPathPattern function in libxslt/pattern.c and (2) the xsltGenerateIdFunction function in libxslt/functions.c.	libxslt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376778
8456	CVE-2012-2845	Medium		Integer overflow in the jpeg_data_load_data function in jpeg-data.c in libjpeg in exif 0.6.20 allows remote attackers to cause a denial of service (buffer over-read and application crash) or obtain potentially sensitive information via a crafted JPEG file.	libexif	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366803
8457	CVE-2012-2841	High		Integer underflow in the exif_entry_get_value function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) 0.6.20 might allow remote attackers to execute arbitrary code via vectors involving a crafted buffer-size parameter during the formatting of an EXIF tag, leading to a heap-based buffer overflow.	libexif	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366809
8458	CVE-2012-2840	High		Off-by-one error in the exif_convert_utf16_to_utf8 function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted EXIF tags in an image.	libexif	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366793
8459	CVE-2012-2837	Medium		The mnote_olympus_entry_get_value function in olympus/mnote-olympus-entry.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service (divide-by-zero error) via an image with crafted EXIF tags that are not properly handled during the formatting of EXIF maker note tags.	libexif	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366798
8460	CVE-2012-2836	Medium		The exif_data_load_data function in exif-data.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from process memory via crafted EXIF tags in an image.	libexif	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366788
8461	CVE-2012-2814	High		Buffer overflow in the exif_entry_format_value function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) 0.6.20 allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted EXIF tags in an image.	libexif	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366817
8462	CVE-2012-2813	Medium		The exif_convert_utf16_to_utf8 function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from process memory via crafted EXIF tags in an image.	libexif	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366808
8463	CVE-2012-2812	Medium		The exif_entry_get_value function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from process memory via crafted EXIF tags in an image.	libexif	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366794
8464	CVE-2012-2807	High		Multiple integer overflows in libxml2, as used in Google Chrome before 20.0.1132.43, on 64-bit Linux platforms allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359309
8465	CVE-2012-2805	Medium	High	Unspecified vulnerability in FFMPEG 0.10 allows remote attackers to cause a denial of service.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5361
8466	CVE-2012-2781			Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2771, CVE-2012-2773, CVE-2012-2778, and CVE-2012-2780.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5005
8467	CVE-2012-2780			Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2771, CVE-2012-2773, CVE-2012-2778, and CVE-2012-2781.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4937
8468	CVE-2012-2779	High		Unspecified vulnerability in the decode_frame function in libavcodec/indeo5.c in FFmpeg before 0.11 has unknown impact and attack vectors, related to an invalid gop header and decoding in a half initialized context.	gst-ffmpeg	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-2119
8469	CVE-2012-2778			Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2771, CVE-2012-2773, CVE-2012-2780, and CVE-2012-2781.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4959
8470	CVE-2012-2773			Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2771, CVE-2012-2778, CVE-2012-2780, and CVE-2012-2781.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5083
8471	CVE-2012-2771			Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2773, CVE-2012-2778, CVE-2012-2780, and CVE-2012-2781.	ffmpeg	Unchanged	Won't Fix	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5025
8472	CVE-2012-2760	Low		mod_auth_openid before 0.7 for Apache uses world-readable permissions for /tmp/mod_auth_openid.db, which allows local users to obtain session ids.	Apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366799
8473	CVE-2012-2750	High		Unspecified vulnerability in MySQL 5.5.x before 5.5.23 has unknown impact and attack vectors related to a Security Fix, aka Bug #59533. NOTE: this might be a duplicate of CVE-2012-1689, but as of 20120816, Oracle has not commented on this possibility.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00373998
8474	CVE-2012-2749	Medium		MySQL 5.1.x before 5.1.63 and 5.5.x before 5.5.24 allows remote authenticated users to cause a denial of service (mysqld crash) via vectors related to incorrect calculation and a sort order index.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374001
8475	CVE-2012-2745	Medium		The copy_creds function in kernel/cred.c in the Linux kernel before 3.3.2 provides an invalid replacement session keyring to a child process, which allows local users to cause a denial of service (panic) via a crafted application that uses the fork system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370214

	A	B	C	D	E	F	G	H	I	J	K	L	M
8476	CVE-2012-2744	High		net/ipv6/netfilter/nf_conntrack_reasm.c in the Linux kernel before 2.6.34, when the nf_conntrack_ipv6 module is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via certain types of fragmented IPv6 packets.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370210
8477	CVE-2012-2741	Medium		Cross-site scripting (XSS) vulnerability in public_html/lists/admin/ in phpList before 2.10.18 allows remote attackers to inject arbitrary web script or HTML via the num parameter in a reconcileusers action.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376776
8478	CVE-2012-2740	High		SQL injection vulnerability in public_html/lists/admin in phpList before 2.10.18 allows remote attackers to execute arbitrary SQL commands via the sortby parameter in a find action.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376782
8479	CVE-2012-2733	Medium		java/org/apache/coyote/http11/InternalNioInputBuffer.java in the HTTP NIO connector in Apache Tomcat 6.x before 6.0.36 and 7.x before 7.0.28 does not properly restrict the request-header size, which allows remote attackers to cause a denial of service (memory consumption) via a large amount of header data.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392078
8480	CVE-2012-2695	High		The Active Record component in Ruby on Rails before 3.0.14, 3.1.x before 3.1.6, and 3.2.x before 3.2.6 does not properly implement the passing of request data to a where method in an ActiveRecord class, which allows remote attackers to conduct certain SQL injection attacks via nested query parameters that leverage improper handling of nested hashes, a related issue to CVE-2012-2661.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359340
8481	CVE-2012-2694	Medium		actionpack/lib/action_dispatch/http/request.rb in Ruby on Rails before 3.0.14, 3.1.x before 3.1.6, and 3.2.x before 3.2.6 does not properly consider differences in parameter handling between the Active Record component and the Rack interface, which allows remote attackers to bypass intended database-query restrictions and perform NULL checks via a crafted request, as demonstrated by certain ['xyz', nil] values, a related issue to CVE-2012-2660.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359318
8482	CVE-2012-2693	Low		libvirt, possibly before 0.9.12, does not properly assign USB devices to virtual machines when multiple devices have the same vendor and product ID, which might cause the wrong device to be associated with a guest and might allow local users to access unintended USB devices.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359306
8483	CVE-2012-2688	High		Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before 5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an overflow.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366812
8484	CVE-2012-2687	Low		Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00373997
8485	CVE-2012-2686	Medium		crypto/evp/e_aes_cbc_hmac_sha1.c in the AES-NI functionality in the TLS 1.1 and 1.2 implementations in OpenSSL 1.0.1 before 1.0.1d allows remote attackers to cause a denial of service (application crash) via crafted CBC data.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00404138
8486	CVE-2012-2677	Medium		Integer overflow in the ordered_malloc function in boost/pool/pool.hpp in Boost Pool before 3.9 makes it easier for context-dependent attackers to perform memory-related attacks such as buffer overflows via a large size value, which causes less memory to be allocated than expected.	boost	Unchanged	8.0.0.4	9.0.0.0	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366777
8487	CVE-2012-2669	Low		The main function in tools/hv/hv_kvp_daemon.c in hypervkvpd, as distributed in the Linux kernel before 3.4.5, does not validate the origin of Netlink messages, which allows local users to spoof Netlink communication via a crafted connector message.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397022
8488	CVE-2012-2668	Medium		libraries/libldap/tls_m.c in OpenLDAP, possibly 2.4.31 and earlier, when using the Mozilla NSS backend, always uses the default cipher suite even when TLSCipherSuite is set, which might cause OpenLDAP to use weaker ciphers than intended and make it easier for remote attackers to obtain sensitive information.	openldap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359348
8489	CVE-2012-2663	High		extensions/libxt_tcp.c in iptables through 1.4.21 does not match TCP SYN+FIN packets in --syn rules, which might allow remote attackers to bypass intended firewall restrictions via crafted packets. NOTE: the CVE-2012-6638 fix makes this issue less relevant.	iptables	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN6-6878
8490	CVE-2012-2661	High		The Active Record component in Ruby on Rails 3.0.x before 3.0.13, 3.1.x before 3.1.5, and 3.2.x before 3.2.4 does not properly implement the passing of request data to a where method in an ActiveRecord class, which allows remote attackers to conduct certain SQL injection attacks via nested query parameters that leverage unintended recursion, a related issue to CVE-2012-2695.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359310
8491	CVE-2012-2660	Medium		actionpack/lib/action_dispatch/http/request.rb in Ruby on Rails before 3.0.13, 3.1.x before 3.1.5, and 3.2.x before 3.2.4 does not properly consider differences in parameter handling between the Active Record component and the Rack interface, which allows remote attackers to bypass intended database-query restrictions and perform NULL checks via a crafted request, as demonstrated by certain [nil] values, a related issue to CVE-2012-2694.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359345

	A	B	C	D	E	F	G	H	I	J	K	L	M
8492	CVE-2012-2655	Medium		PostgreSQL 8.3.x before 8.3.19, 8.4.x before 8.4.12, 9.0.x before 9.0.8, and 9.1.x before 9.1.4 allows remote authenticated users to cause a denial of service (server crash) by adding the (1) SECURITY DEFINER or (2) SET attributes to a procedural language's call handler.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366790
8493	CVE-2012-2652	Medium		The bdrv_open function in Qemu 1.0 does not properly handle the failure of the mkstemp function, when in snapshot node, which allows local users to overwrite or read arbitrary files via a symlink attack on an unspecified temporary file.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370229
8494	CVE-2012-2633	Medium		Cross-site scripting (XSS) vulnerability in wassup.php in the WassUp plugin before 1.8.3.1 for WordPress allows remote attackers to inject arbitrary web script or HTML via the User-Agent HTTP header.	plugin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359303
8495	CVE-2012-2390	Medium		Memory leak in mm/hugetlb.c in the Linux kernel before 3.4.2 allows local users to cause a denial of service (memory consumption or system crash) via invalid MAP_HUGETLB mmap operations.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355892
8496	CVE-2012-2389	Low		hostapd 0.7.3, and possibly other versions before 1.0, uses 0644 permissions for /etc/hostapd/hostapd.conf, which might allow local users to obtain sensitive information such as credentials.	hostapd	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359332
8497	CVE-2012-2388	High		The GMP Plugin in strongSwan 4.2.0 through 4.6.3 allows remote attackers to bypass authentication via a (1) empty or (2) zeroed RSA signature, aka RSA signature verification vulnerability.	strongswan	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413582
8498	CVE-2012-2386	High		Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362915
8499	CVE-2012-2384	Medium		Integer overflow in the i915_gem_do_execbuffer function in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the Direct Rendering Manager (DRM) subsystem in the Linux kernel before 3.3.5 on 32-bit platforms allows local users to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355887
8500	CVE-2012-2383	Medium		Integer overflow in the i915_gem_execbuffer2 function in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the Direct Rendering Manager (DRM) subsystem in the Linux kernel before 3.3.5 on 32-bit platforms allows local users to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355899
8501	CVE-2012-2381	Low		Multiple cross-site scripting (XSS) vulnerabilities in Apache Roller before 5.0.1 allow remote authenticated users to inject arbitrary web script or HTML by leveraging the blogger role.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359321
8502	CVE-2012-2380	High		Multiple cross-site request forgery (CSRF) vulnerabilities in the admin/editor console in Apache Roller before 5.0.1 allow remote attackers to hijack the authentication of admins or editors by leveraging the HTTP POST functionality.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359333
8503	CVE-2012-2379	High		Apache CXF 2.4.x before 2.4.8, 2.5.x before 2.5.4, and 2.6.x before 2.6.1, when a Supporting Token specifies a child WS-SecurityPolicy 1.1 or 1.2 policy, does not properly ensure that an XML element is signed or encrypted, which has unspecified impact and attack vectors.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399171
8504	CVE-2012-2378	Medium		Apache CXF 2.4.5 through 2.4.7, 2.5.1 through 2.5.3, and 2.6.x before 2.6.1, does not properly enforce child policies of a WS-SecurityPolicy 1.1 SupportingToken policy on the client side, which allows remote attackers to bypass the (1) AlgorithmSuite, (2) SignedParts, (3) SignedElements, (4) EncryptedParts, and (5) EncryptedElements policies.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00399176
8505	CVE-2012-2376	High		Buffer overflow in the com_print_typeinfo function in PHP 5.4.3 and earlier on Windows allows remote attackers to execute arbitrary code via crafted arguments that trigger incorrect handling of COM object VARIANT types, as exploited in the wild in May 2012.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353054
8506	CVE-2012-2375	Medium		The __nfs4_get_acl_uncached function in fs/nfs/nfs4proc.c in the NFSv4 implementation in the Linux kernel before 3.3.2 uses an incorrect length variable during a copy operation, which allows remote NFS servers to cause a denial of service (OOPS) by sending an excessive number of bitmap words in an FATTR4_ACL reply. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-4131.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355878
8507	CVE-2012-2373	Medium		The Linux kernel before 3.4.5 on the x86 platform, when Physical Address Extension (PAE) is enabled, does not properly use the Page Middle Directory (PMD), which allows local users to cause a denial of service (panic) via a crafted application that triggers a race condition.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370211
8508	CVE-2012-2372	Medium		The rds_ib_xmit function in net/rds/ib_send.c in the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel 3.7.4 and earlier allows local users to cause a denial of service (BUG_ON and kernel panic) by establishing an RDS connection with the source IP address equal to the IPoIB interface's own IP address, as demonstrated by rds-ping.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402357
8509	CVE-2012-2370	Medium		Multiple integer overflows in the read_bitmap_file_data function in io-xbm.c in gdk-pixbuf before 2.26.1 allow remote attackers to cause a denial of service (application crash) via a negative (1) height or (2) width in an XBM file, which triggers a heap-based buffer overflow.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374008

	A	B	C	D	E	F	G	H	I	J	K	L	M
8510	CVE-2012-2337	High		sudo 1.6.x and 1.7.x before 1.7.9p1, and 1.8.x before 1.8.4p5, does not properly support configurations that use a netmask syntax, which allows local users to bypass intended command restrictions in opportunistic circumstances by executing a command on a host that has an IPv4 address.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353049
8511	CVE-2012-2336	Medium		sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to cause a denial of service (resource consumption) by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'T' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349741
8512	CVE-2012-2335	High		php-wrapper.fcgi does not properly handle command-line arguments, which allows remote attackers to bypass a protection mechanism in PHP 5.3.12 and 5.4.2 and execute arbitrary code by leveraging improper interaction between the PHP sapi/cgi/cgi_main.c component and a query string beginning with a +- sequence.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349745
8513	CVE-2012-2334	Medium		Integer overflow in filter/source/msfilter/msdffimp.cxx in OpenOffice.org (OOo) 3.3, 3.4 Beta, and possibly earlier, and LibreOffice before 3.5.3, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the length of an Escher graphics record in a PowerPoint (.ppt) document, which triggers a buffer overflow.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359351
8514	CVE-2012-2333	Medium		Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353057
8515	CVE-2012-2329	Medium		Buffer overflow in the apache_request_headers function in sapi/cgi/cgi_main.c in PHP 5.4.x before 5.4.3 allows remote attackers to cause a denial of service (application crash) via a long string in the header of an HTTP request.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349744
8516	CVE-2012-2319	High		Multiple buffer overflows in the hfsplus filesystem implementation in the Linux kernel before 3.3.5 allow local users to gain privileges via a crafted HFS plus filesystem, a related issue to CVE-2009-4020.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353051
8517	CVE-2012-2317	Medium		The Debian php_crypt_revamped.patch patch for PHP 5.3.x, as used in the php5 package before 5.3.3-7+squeeze4 in Debian GNU/Linux squeeze, the php5 package before 5.3.2-1ubuntu4.17 in Ubuntu 10.04 LTS, and the php5 package before 5.3.5-1ubuntu7.10 in Ubuntu 11.04, does not properly handle an empty salt string, which might allow remote attackers to bypass authentication by leveraging an application that relies on the PHP crypt function to choose a salt for password hashing.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370221
8518	CVE-2012-2313	Low		The rio_ioctl function in drivers/net/ethernet/dlink/dl2k.c in the Linux kernel before 3.3.7 does not restrict access to the SIOCSMIIREG command, which allows local users to write data to an Ethernet adapter via an ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355889
8519	CVE-2012-2311	High		sapi/cgi/cgi_main.c in PHP before 5.3.13 and 5.4.x before 5.4.3, when configured as a CGI script (aka php-cgi), does not properly handle query strings that contain a %3D sequence but no = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1823.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349740
8520	CVE-2012-2192	Medium		The socketpair function in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.1.4-FP-25 SP-02 allows local users to cause a denial of service (system crash) via a crafted application that leverages the presence of a socket on the free list.	aix	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359315
8521	CVE-2012-2179	Medium		libodm.a in IBM AIX 5.3, 6.1, and 7.1 allows local users to overwrite arbitrary files via a symlink attack on a temporary file.	aix	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359353
8522	CVE-2012-2152	High		Stack-based buffer overflow in the get_packet method in socket.c in dhcpcd 3.2.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long packet.	dhcp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366785
8523	CVE-2012-2150	Medium		xfs_metadump in xfsprogs before 3.2.4 does not properly obfuscate file data, which allows remote attackers to obtain sensitive information by reading a generated image.	xfsprogs	Unchanged	8.0.0.4	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-774
8524	CVE-2012-2149	High		The WPXContentListener::_closeTableRow function in WPXContentListener.cpp in libwpd 0.8.8, as used by OpenOffice.org (OOo) before 3.4, allows remote attackers to execute arbitrary code via a crafted Wordperfect .WPD document that causes a negative array index to be used. NOTE: some sources report this issue as an integer overflow.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359319
8525	CVE-2012-2143	Medium		The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362926

	A	B	C	D	E	F	G	H	I	J	K	L	M
8526	CVE-2012-2141	Low		Array index error in the handle_nsExtendOutput2Table function in agent/mibgroup/agent/extend.c in Net-SNMP 5.7.1 allows remote authenticated users to cause a denial of service (out-of-bounds read and snmpd crash) via an SNMP GET request for an entry not in the extension table.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00373995
8527	CVE-2012-2140	High		The Mail gem before 2.4.3 for Ruby allows remote attackers to execute arbitrary commands via shell metacharacters in a (1) sendmail or (2) exim delivery.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366814
8528	CVE-2012-2139	Medium		Directory traversal vulnerability in lib/mail/network/delivery_methods/file_delivery.rb in the Mail gem before 2.4.3 for Ruby allows remote attackers to read arbitrary files via a .. (dot dot) in the to parameter.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366811
8529	CVE-2012-2138	Medium		The @CopyFrom operation in the POST servlet in the org.apache.sling.servlets.post bundle before 2.1.2 in Apache Sling does not prevent attempts to copy an ancestor node to a descendant node, which allows remote attackers to cause a denial of service (infinite loop) via a crafted HTTP request.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362920
8530	CVE-2012-2137	Medium		Buffer overflow in virt/kvm/irq_comm.c in the KVM subsystem in the Linux kernel before 3.2.24 allows local users to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to Message Signaled Interrupts (MSI), irq routing entries, and an incorrect check by the setup_routing_entry function before invoking the kvm_set_irq function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402355
8531	CVE-2012-2136	High		The sock_alloc_send_pskb function in net/core/sock.c in the Linux kernel before 3.4.5 does not properly validate a certain length value, which allows local users to cause a denial of service (heap-based buffer overflow and system crash) or possibly gain privileges by leveraging access to a TUN/TAP device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370212
8532	CVE-2012-2135	Medium		The utf-16 decoder in Python 3.1 through 3.3 does not update the aligned_end variable after calling the unicode_decode_call_errorhandler function, which allows remote attackers to obtain sensitive information (process memory) or cause a denial of service (memory corruption and crash) via unspecified vectors.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374015
8533	CVE-2012-2133	Medium		Use-after-free vulnerability in the Linux kernel before 3.3.6, when huge pages are enabled, allows local users to cause a denial of service (system crash) or possibly gain privileges by interacting with a hugetlbfs filesystem, as demonstrated by a umount operation that triggers improper handling of quota data.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362917
8534	CVE-2012-2132	Medium		libsoup 2.32.2 and earlier does not validate certificates or clear the trust flag when the ssl-ca-file does not exist, which allows remote attackers to bypass authentication by connecting with a SSL connection.	libsoup	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374007
8535	CVE-2012-2131	High		Multiple integer signedness errors in crypto/buffer/buffer.c in OpenSSL 0.9.8v allow remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-2110.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347673
8536	CVE-2012-2127	Medium		fs/proc/root.c in the procfs implementation in the Linux kernel before 3.2 does not properly interact with CLONE_NEWPID clone system calls, which allows remote attackers to cause a denial of service (reference leak and memory consumption) by making many connections to a daemon that uses PID namespaces to isolate clients, as demonstrated by vsftpd.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359323
8537	CVE-2012-2123	High		The cap_bprm_set_creds function in security/commoncap.c in the Linux kernel before 3.3.3 does not properly handle the use of file system capabilities (aka fcaps) for implementing a privileged executable file, which allows local users to bypass intended personality restrictions via a crafted application, as demonstrated by an attack that uses a parent process to disable ASLR.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353046
8538	CVE-2012-2122	Medium		sql/password.c in Oracle MySQL 5.1.x before 5.1.63, 5.5.x before 5.5.24, and 5.6.x before 5.6.6, and MariaDB 5.1.x before 5.1.62, 5.2.x before 5.2.12, 5.3.x before 5.3.6, and 5.5.x before 5.5.23, when running in certain environments with certain implementations of the memcmp function, allows remote attackers to bypass authentication by repeatedly authenticating with the same incorrect password, which eventually causes a token comparison to succeed due to an improperly-checked return value.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359338
8539	CVE-2012-2121	Medium		The KVM implementation in the Linux kernel before 3.3.4 does not properly manage the relationships between memory slots and the iommu, which allows guest OS users to cause a denial of service (host OS crash) by leveraging administrative access to the guest OS to conduct hotunplug and hotplug operations on devices.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353067
8540	CVE-2012-2119	Medium		Buffer overflow in the macvtap device driver in the Linux kernel before 3.4.5, when running in certain configurations, allows privileged KVM guest users to cause a denial of service (crash) via a long descriptor with a long vector length.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402358
8541	CVE-2012-2118	High		Format string vulnerability in the LogVHdrMessageVerb function in os/log.c in X.Org X11 1.11 allows attackers to cause a denial of service or possibly execute arbitrary code via format string specifiers in an input device name.	xorg-x11	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353055

	A	B	C	D	E	F	G	H	I	J	K	L	M
8542	CVE-2012-2113	Medium		Multiple integer overflows in tiff2pdf in libtiff before 4.0.2 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tiff image, which triggers a heap-based buffer overflow.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366781
8543	CVE-2012-2111	Medium		The (1) CreateAccount, (2) OpenAccount, (3) AddAccountRights, and (4) RemoveAccountRights LSA RPC procedures in smbd in Samba 3.4.x before 3.4.17, 3.5.x before 3.5.15, and 3.6.x before 3.6.5 do not properly restrict modifications to the privileges database, which allows remote authenticated users to obtain the take ownership privilege via an LSA connection.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349746
8544	CVE-2012-2110	High		The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347671
8545	CVE-2012-2102	Low		MySQL 5.1.x before 5.1.62 and 5.5.x before 5.5.22 allows remote authenticated users to cause a denial of service (assertion failure and mysqld abort) by deleting a record and using HANDLER READ NEXT.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374014
8546	CVE-2012-2100	High		The ext4_fill_flex_info function in fs/ext4/super.c in the Linux kernel before 3.2.2, on the x86 platform and unspecified other platforms, allows user-assisted remote attackers to trigger inconsistent filesystem-groups data and possibly cause a denial of service via a malformed ext4 filesystem containing a super block with a large FLEX_BG group size (aka s_log_groups_per_flex value). NOTE: this vulnerability exists because of an incomplete fix for CVE-2009-4307.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362918
8547	CVE-2012-2098	Medium		Algorithmic complexity vulnerability in the sorting algorithms in bzip2 compressing stream (BZip2CompressorOutputStream) in Apache Commons Compress before 1.4.1 allows remote attackers to cause a denial of service (CPU consumption) via a file with many repeating inputs.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362927
8548	CVE-2012-2088	High		Integer signedness error in the TIFFReadDirectory function in tif_dirread.c in libtiff 3.9.4 and earlier allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a negative tile depth in a tiff image, which triggers an improper conversion between signed and unsigned types, leading to a heap-based buffer overflow.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366800
8549	CVE-2012-1912	Medium		Cross-site scripting (XSS) vulnerability in preferences.php in PHP Address Book 7.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the from parameter. NOTE: the index.php vector is already covered by CVE-2008-2566.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376785
8550	CVE-2012-1911	High		Multiple SQL injection vulnerabilities in PHP Address Book 6.2.12 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) to_group parameter to group.php or (2) id parameter to vcard.php. NOTE: the edit.php vector is already covered by CVE-2008-2565.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376780
8551	CVE-2012-1823	High		sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349743
8552	CVE-2012-1820	Low		The bgp_capability_orf function in bgpd in Quagga 0.99.20.1 and earlier allows remote attackers to cause a denial of service (assertion failure and daemon exit) by leveraging a BGP peering relationship and sending a malformed Outbound Route Filtering (ORF) capability TLV in an OPEN message.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355897
8553	CVE-2012-1798	Medium		The TIFFGetEXIFProperties function in coders/tiff.c in ImageMagick before 6.7.6-3 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted EXIF IFD in a TIFF image.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355884
8554	CVE-2012-1757	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366778
8555	CVE-2012-1756	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.23 and earlier allows remote authenticated users to affect availability via unknown vectors.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366791
8556	CVE-2012-1735	Medium		Unspecified vulnerability in Oracle MySQL Server 5.5.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366797
8557	CVE-2012-1734	Medium		Unspecified vulnerability in Oracle MySQL Server 5.1.62 and earlier, and 5.5.23 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366801
8558	CVE-2012-1705	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402346
8559	CVE-2012-1703	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.61 and earlier, and 5.5.21 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349739
8560	CVE-2012-1702	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote attackers to affect availability via unknown vectors.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402353

	A	B	C	D	E	F	G	H	I	J	K	L	M
8561	CVE-2012-1699	Low		The ProcSetEventMask function in difs/events.c in the xfs font server for X.Org X11R6 through X11R6.6 and XFree86 before 3.3.3 calls the SendErrToClient function with a mask value instead of a pointer, which allows local users to cause a denial of service (memory corruption and crash) or obtain potentially sensitive information from memory via a SetEventMask request that triggers an invalid pointer dereference.	xorg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397025
8562	CVE-2012-1697	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.21 and earlier allows remote authenticated users to affect availability via unknown vectors related to Partition.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349749
8563	CVE-2012-1696	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.19 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349735
8564	CVE-2012-1690	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.61 and earlier, and 5.5.21 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349748
8565	CVE-2012-1689	Medium		Unspecified vulnerability in Oracle MySQL Server 5.1.62 and earlier, and 5.5.22 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366783
8566	CVE-2012-1688	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.61 and earlier, and 5.5.21 and earlier, allows remote authenticated users to affect availability, related to Server DML.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349742
8567	CVE-2012-1667	High		ISC BIND 9.x before 9.7.6-P1, 9.8.x before 9.8.3-P1, 9.9.x before 9.9.1-P1, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P1 does not properly handle resource records with a zero-length RDATA section, which allows remote DNS servers to cause a denial of service (daemon crash or data corruption) or obtain sensitive information from process memory via a crafted record.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355891
8568	CVE-2012-1663	High		Double free vulnerability in libgnutls in GnuTLS before 3.0.14 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted certificate list.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00339922
8569	CVE-2012-1618	High		Interaction error in the PostgreSQL JDBC driver before 8.2, when used with a PostgreSQL server with the standard_conforming_strings option enabled, such as the default configuration of PostgreSQL 9.1, does not properly escape unspecified JDBC statement parameters, which allows remote attackers to perform SQL injection attacks. NOTE: as of 20120330, it was claimed that the upstream developer planned to dispute this issue, but an official dispute has not been posted as of 20121005.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382767
8570	CVE-2012-1610	Medium		Integer overflow in the GetEXIFProperty function in magick/property.c in ImageMagick before 6.7.6-4 allows remote attackers to cause a denial of service (out-of-bounds read) via a large component count for certain EXIF tags in a JPEG image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0259.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355894
8571	CVE-2012-1601	Medium		The KVM implementation in the Linux kernel before 3.3.6 allows host OS users to cause a denial of service (NULL pointer dereference and host OS crash) by making a KVM_CREATE_IRQCHIP ioctl call after a virtual CPU already exists.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353061
8572	CVE-2012-1583	Medium		Double free vulnerability in the xfrm6_tunnel_rcv function in net/ipv6/xfrm6_tunnel.c in the Linux kernel before 2.6.22, when the xfrm6_tunnel module is enabled, allows remote attackers to cause a denial of service (panic) via crafted IPv6 packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359322
8573	CVE-2012-1573	Medium		gnutls_cipher.c in libgnutls in GnuTLS before 2.12.17 and 3.x before 3.0.15 does not properly handle data encrypted with a block cipher, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) via a crafted record, as demonstrated by a crafted GenericBlockCipher structure.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00343366
8574	CVE-2012-1569	Medium		The asn1_get_length_der function in decoding.c in GNU Libtasn1 before 2.12, as used in GnuTLS before 3.0.16 and other products, does not properly handle certain large length values, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly have unspecified other impact via a crafted ASN.1 structure.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00343363
8575	CVE-2012-1190	Medium		Cross-site scripting (XSS) vulnerability in the replication-setup functionality in js/replication.js in phpMyAdmin 3.4.x before 3.4.10.1 allows user-assisted remote attackers to inject arbitrary web script or HTML via a crafted database name.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349736
8576	CVE-2012-1186	Medium		Integer overflow in the SyncImageProfiles function in profile.c in ImageMagick 6.7.5-8 and earlier allows remote attackers to cause a denial of service (infinite loop) via crafted IOP tag offsets in the IFD in an image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0248.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355873
8577	CVE-2012-1185	High		Multiple integer overflows in (1) magick/profile.c or (2) magick/property.c in ImageMagick 6.7.5 and earlier allow remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via crafted offset value in the ResolutionUnit tag in the EXIF IFD0 of an image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0247.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355882

	A	B	C	D	E	F	G	H	I	J	K	L	M
8578	CVE-2012-1182	High		The RPC code generator in Samba 3.x before 3.4.16, 3.5.x before 3.5.14, and 3.6.x before 3.6.4 does not implement validation of an array length in a manner consistent with validation of array memory allocation, which allows remote attackers to execute arbitrary code via a crafted RPC call.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00345314
8579	CVE-2012-1181	Medium		fcgid_spawn_ctl.c in the mod_fcgid module 2.3.6 for the Apache HTTP Server does not recognize the FcgidMaxProcessesPerClass directive for a virtual host, which makes it easier for remote attackers to cause a denial of service (memory consumption) via a series of HTTP requests that triggers a process count higher than the intended limit.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00343414
8580	CVE-2012-1179	Medium		The Linux kernel before 3.3.1, when KVM is used, allows guest OS users to cause a denial of service (host OS crash) by leveraging administrative access to the guest OS, related to the pmd_none_or_clear_bad function and page faults for huge pages.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353066
8581	CVE-2012-1177	Medium		libgdata before 0.10.2 and 0.11.x before 0.11.1 does not validate SSL certificates, which allows remote attackers to obtain user names and passwords via a man-in-the-middle (MITM) attack with a spoofed certificate.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374013
8582	CVE-2012-1173	Medium		Multiple integer overflows in tiff_getimage.c in LibTIFF 3.9.4 allow remote attackers to execute arbitrary code via a crafted tile size in a TIFF file, which is not properly handled by the (1) gtTileSeparate or (2) gtStripSeparate function, leading to a heap-based buffer overflow.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355888
8583	CVE-2012-1172	Medium		The file-upload implementation in rfc1867.c in PHP before 5.4.0 does not properly handle invalid [(open square bracket) characters in name values, which makes it easier for remote attackers to cause a denial of service (malformed $_FILES indexes) or conduct directory traversal attacks during multi-file uploads by leveraging a script that lacks its own filename restrictions.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353047
8584	CVE-2012-1171	Medium		The libxml RSHUTDOWN function in PHP 5.x allows remote attackers to bypass the open_basedir protection mechanism and read arbitrary files via vectors involving a stream_close method call during use of a custom stream wrapper.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6871
8585	CVE-2012-1165	Medium		The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before 1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00343415
8586	CVE-2012-1164	Low		slapd in OpenLDAP before 2.4.30 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via an LDAP search query with attrsOnly set to true, which causes empty attributes to be returned.	openldap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362912
8587	CVE-2012-1151	Medium		Multiple format string vulnerabilities in dbdimp.c in DBD::Pg (aka DBD-Pg or libdbd-pg-perl) module before 2.19.0 for Perl allow remote PostgreSQL database servers to cause a denial of service (process crash) via format string specifiers in (1) a crafted database warning to the pg_warn function or (2) a crafted DBD statement to the dbd_st_prepare function.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376787
8588	CVE-2012-1150	Medium		Python before 2.6.8, 2.7.x before 2.7.3, 3.x before 3.1.5, and 3.2.x before 3.2.3 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table.	python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382745
8589	CVE-2012-1149	High		Integer overflow in the vclmi.dll module in OpenOffice.org (OOo) 3.3, 3.4 Beta, and possibly earlier, and LibreOffice before 3.5.3, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted embedded image object, as demonstrated by a JPEG image in a .DOC file, which triggers a heap-based buffer overflow.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359334
8590	CVE-2012-1148	Medium		Memory leak in the poolGrow function in expat/lib/xmlparse.c in expat before 2.1.0 allows context-dependent attackers to cause a denial of service (memory consumption) via a large number of crafted XML files that cause improperly-handled reallocation failures when expanding entities.	expat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362928
8591	CVE-2012-1147	Medium		readfilemap.c in expat before 2.1.0 allows context-dependent attackers to cause a denial of service (file descriptor consumption) via a large number of crafted XML files.	expat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362916
8592	CVE-2012-1146	High		The mem_cgroup_usage_unregister_event function in mm/memcontrol.c in the Linux kernel before 3.2.10 does not properly handle multiple events that are attached to the same eventfd, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by registering memory threshold events.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353068
8593	CVE-2012-1144	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via a crafted TrueType font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347679
8594	CVE-2012-1143	Medium		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347661

	A	B	C	D	E	F	G	H	I	J	K	L	M
8595	CVE-2012-1142	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via crafted glyph-outline data in a font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347666
8596	CVE-2012-1141	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via a crafted ASCII string in a BDF font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347669
8597	CVE-2012-1140	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via a crafted PostScript font object.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347681
8598	CVE-2012-1139	High		Array index error in FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid stack read operation and memory corruption) or possibly execute arbitrary code via crafted glyph data in a BDF font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347678
8599	CVE-2012-1138	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via vectors involving the MIRP instruction in a TrueType font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347667
8600	CVE-2012-1137	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via a crafted header in a BDF font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347659
8601	CVE-2012-1136	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via crafted glyph or bitmap data in a BDF font that lacks an ENCODING field.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347662
8602	CVE-2012-1135	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via vectors involving the NPUSHB and NPUSHW instructions in a TrueType font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347680
8603	CVE-2012-1134	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via crafted private-dictionary data in a Type 1 font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347670
8604	CVE-2012-1133	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via crafted glyph or bitmap data in a BDF font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347663
8605	CVE-2012-1132	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted dictionary data in a Type 1 font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347677
8606	CVE-2012-1131	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, on 64-bit platforms allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via vectors related to the cell table of a font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347672
8607	CVE-2012-1130	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted property data in a PCF font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347660
8608	CVE-2012-1129	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via a crafted SFNT string in a Type 42 font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347676
8609	CVE-2012-1128	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (NULL pointer dereference and memory corruption) or possibly execute arbitrary code via a crafted TrueType font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347665
8610	CVE-2012-1127	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted glyph or bitmap data in a BDF font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347674
8611	CVE-2012-1126	High		FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted property data in a BDF font.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347668
8612	CVE-2012-1097	High		The regset (aka register set) feature in the Linux kernel before 3.2.10 does not properly handle the absence of .get and .set methods, which allows local users to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via a (1) PTRACE_GETREGSET or (2) PTRACE_SETREGSET ptrace call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353059

	A	B	C	D	E	F	G	H	I	J	K	L	M
8613	CVE-2012-1090	Medium		The cifs_lookup function in fs/cifs/dir.c in the Linux kernel before 3.2.10 allows local users to cause a denial of service (OOPS) via attempted access to a special file, as demonstrated by a FIFO.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353053
8614	CVE-2012-1089	Medium		Directory traversal vulnerability in Apache Wicket 1.4.x before 1.4.20 and 1.5.x before 1.5.5 allows remote attackers to read arbitrary web-application files via a relative pathname in a URL for a Wicket resource that corresponds to a null package.	apache wicket	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00343360
8615	CVE-2012-1088	Low		iproute2 before 3.3.0 allows local users to overwrite arbitrary files via a symlink attack on a temporary file used by (1) configure or (2) examples/dhcp-client-script.	iproute2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6872
8616	CVE-2012-1016	Medium		The pkinit_server_return_padata function in plugins/preauth/pkinit/pkinit_srv.c in the PKINIT implementation in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.10.4 attempts to find an agility KDF identifier in inappropriate circumstances, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted Draft 9 request.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413574
8617	CVE-2012-1015	High		The kdc_handle_protected_negotiation function in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.8.x, 1.9.x before 1.9.5, and 1.10.x before 1.10.3 attempts to calculate a checksum before verifying that the key type is appropriate for a checksum, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free, heap memory corruption, and daemon crash) via a crafted AS-REQ request.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413560
8618	CVE-2012-1014	High		The process_as_req function in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.10.x before 1.10.3 does not initialize a certain structure member, which allows remote attackers to cause a denial of service (uninitialized pointer dereference and daemon crash) or possibly execute arbitrary code via a malformed AS-REQ request.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413544
8619	CVE-2012-1013	Medium		The check_1_6_dummy function in lib/kadm5/srv/svr_principal.c in kadmind in MIT Kerberos 5 (aka krb5) 1.8.x, 1.9.x, and 1.10.x before 1.10.2 allows remote authenticated administrators to cause a denial of service (NULL pointer dereference and daemon crash) via a KRB5_KDB_DISALLOW_ALL_TIX create request that lacks a password.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413583
8620	CVE-2012-1012	Medium		server/server_stubs.c in the kadmin protocol implementation in MIT Kerberos 5 (aka krb5) 1.10 before 1.10.1 does not properly restrict access to (1) SET_STRING and (2) GET_STRINGS operations, which might allow remote authenticated administrators to modify or read string attributes by leveraging the global list privilege.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413591
8621	CVE-2012-1007	Medium		Multiple cross-site scripting (XSS) vulnerabilities in Apache Struts 1.3.10 allow remote attackers to inject arbitrary web script or HTML via (1) the name parameter to struts-examples/upload/upload-submit.do, or the message parameter to (2) struts-cookbook/processSimple.do or (3) struts-cookbook/processDyna.do.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334412
8622	CVE-2012-1006	Medium		Multiple cross-site scripting (XSS) vulnerabilities in Apache Struts 2.0.14 and 2.2.3 allow remote attackers to inject arbitrary web script or HTML via the (1) name or (2) lastName parameter to struts2-showcase/person/editPerson.action, or the (3) clientName parameter to struts2-rest-showcase/orders.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334413
8623	CVE-2012-0957	Medium		The override_release function in kernel/sys.c in the Linux kernel before 3.4.16 allows local users to obtain sensitive information from kernel stack memory via a uname system call in conjunction with a UNAME26 personality.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397032
8624	CVE-2012-0950	Medium		The Apport hook (DistUpgradeApport.py) in Update Manager, as used by Ubuntu 12.04 LTS, 11.10, and 11.04, uploads the /var/log/dist-upgrade directory when reporting bugs to Launchpad, which allows remote attackers to read repository credentials by viewing a public bug report. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0949.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359342
8625	CVE-2012-0920	High		Use-after-free vulnerability in Dropbear SSH Server 0.52 through 2012.54, when command restriction and public key authentication are enabled, allows remote authenticated users to execute arbitrary code and bypass command restrictions via multiple crafted command requests, related to channels concurrency.	dropbear	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349271
8626	CVE-2012-0884	Medium		The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00339930
8627	CVE-2012-0883	Medium		envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347675

	A	B	C	D	E	F	G	H	I	J	K	L	M
8628	CVE-2012-0882	High		Buffer overflow in yaSSL, as used in MySQL 5.5.20 and possibly other versions including 5.5.x before 5.5.22 and 5.1.x before 5.1.62, allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by VulnDisco Pack Professional 9.17. NOTE: as of 20120224, this disclosure has no actionable information. However, because the module author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes. NOTE: due to lack of details, it is not clear whether this issue is a duplicate of CVE-2012-0492 or another CVE.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397017
8629	CVE-2012-0880			Apache Xerces-C++ allows remote attackers to cause a denial of service (CPU consumption) via a crafted message sent to an XML service that causes hash table collisions.	xerces	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-5024
8630	CVE-2012-0879	Medium		The I/O implementation for block devices in the Linux kernel before 2.6.33 does not properly handle the CLONE_IO feature, which allows local users to cause a denial of service (I/O instability) by starting multiple processes that share an I/O context.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353048
8631	CVE-2012-0878	Medium		Paste Script 1.7.5 and earlier does not properly set group memberships during execution with root privileges, which might allow remote attackers to bypass intended file-access restrictions by leveraging a web application that uses the local filesystem.	pythonpaste	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349738
8632	CVE-2012-0876	Medium		The XML parser (xmlparse.c) in expat before 2.1.0 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via an XML file with many identifiers with the same value.	expat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362924
8633	CVE-2012-0875	Medium		SystemTap 1.7, 1.6.7, and probably other versions, when unprivileged mode is enabled, allows local users to obtain sensitive information from kernel memory or cause a denial of service (kernel panic and crash) via vectors related to crafted DWARF data, which triggers a read of an invalid pointer.	systemtap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6785
8634	CVE-2012-0868	High		CRLF injection vulnerability in pg_dump in PostgreSQL 8.3.x before 8.3.18, 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 allows user-assisted remote attackers to execute arbitrary SQL commands via a crafted file containing object names with newlines, which are inserted into an SQL script that is used when the database is restored.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366795
8635	CVE-2012-0867	Medium		PostgreSQL 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 truncates the common name to only 32 characters when verifying SSL certificates, which allows remote attackers to spoof connections when the host name is exactly 32 characters.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366784
8636	CVE-2012-0866	Medium		CREATE TRIGGER in PostgreSQL 8.3.x before 8.3.18, 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 does not properly check the execute permission for trigger functions marked SECURITY DEFINER, which allows remote authenticated users to execute otherwise restricted triggers on arbitrary data by installing the trigger on an attacker-owned table.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366816
8637	CVE-2012-0864	Medium		Integer overflow in the vfprintf function in stdio-common/vfprintf.c in glibc 2.14 and other versions allows context-dependent attackers to bypass the FORTIFY_SOURCE protection mechanism, conduct format string attacks, and write to arbitrary memory via a large number of arguments.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417548
8638	CVE-2012-0862	Medium		builtins.c in Xinetd before 2.3.15 does not check the service type when the tcpmux-server service is enabled, which exposes all enabled services and allows remote attackers to bypass intended access restrictions via a request to tcpmux port 1.	xinetd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355866
8639	CVE-2012-0845	Medium		SimpleXMLRPCServer.py in SimpleXMLRPCServer in Python before 2.6.8, 2.7.x before 2.7.3, 3.x before 3.1.5, and 3.2.x before 3.2.3 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via an XML-RPC POST request that contains a smaller amount of data than specified by the Content-Length header.	python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382746
8640	CVE-2012-0841	Medium		libxml2 before 2.8.0 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00358693
8641	CVE-2012-0840	Medium		tables/apr_hash.c in the Apache Portable Runtime (APR) library through 1.4.5 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334407
8642	CVE-2012-0831	High		PHP before 5.3.10 does not properly perform a temporary change to the magic_quotes_gpc directive during the importing of environment variables, which makes it easier for remote attackers to conduct SQL injection attacks via a crafted request, related to main/php_variables.c, sapi/cgi/cgi_main.c, and sapi/fpm/fpm/fpm_main.c.	php.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334406
8643	CVE-2012-0830	High		The php_register_variable_ex function in php_variables.c in PHP 5.3.9 allows remote attackers to execute arbitrary code via a request containing a large number of variables, related to improper handling of array variables. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-4885.	php.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334416
8644	CVE-2012-0817	Medium		Memory leak in smbd in Samba 3.6.x before 3.6.3 allows remote attackers to cause a denial of service (memory and CPU consumption) by making many connection requests.	samba.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334441

	A	B	C	D	E	F	G	H	I	J	K	L	M
8645	CVE-2012-0815	Medium		The headerVerifyInfo function in lib/header.c in RPM before 4.9.1.3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a negative value in a region offset of a package header, which is not properly handled in a numeric range comparison.	rpm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355886
8646	CVE-2012-0814	Low		The auth_parse_options function in auth-options.c in sshd in OpenSSH before 5.7 provides debug messages containing authorized_keys command options, which allows remote authenticated users to obtain potentially sensitive information by reading these messages, as demonstrated by the shared user account required by Gitolite. NOTE: this can cross privilege boundaries because a user account may intentionally have no shell or filesystem access, and therefore may have no supported way to read an authorized_keys file in its own home directory.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332174
8647	CVE-2012-0809	High		Format string vulnerability in the sudo_debug function in Sudo 1.8.0 through 1.8.3p1 allows local users to execute arbitrary code via format string sequences in the program name for sudo.	sudo.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334438
8648	CVE-2012-0789	Medium		Memory leak in the timezone functionality in PHP before 5.3.9 allows remote attackers to cause a denial of service (memory consumption) by triggering many strtotime function calls, which are not properly handled by the php_date_parse_tzfile cache.	php.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334391
8649	CVE-2012-0788	Medium		The PDORow implementation in PHP before 5.3.9 does not properly interact with the session feature, which allows remote attackers to cause a denial of service (application crash) via a crafted application that uses a PDO driver for a fetch and then calls the session_start function, as demonstrated by a crash of the Apache HTTP Server.	php.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334403
8650	CVE-2012-0787	Low		The clone_file function in transfer.c in Augeas before 1.0.0, when copy_if_rename_fails is set and EXDEV or EBUSY is returned by the rename function, allows local users to overwrite arbitrary files and obtain sensitive information via a bind mount on the (1) .augsave or (2) destination file when using the backup save option, or (3) .augnew file when using the newfile save option.	augeas	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445861
8651	CVE-2012-0786	Low		The transform_save function in transform_save in Augeas before 1.0.0 allows local users to overwrite arbitrary files and obtain sensitive information via a symlink attack on a .augnew file.	augeas	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00445872
8652	CVE-2012-0698	Medium		tcsd in TrouSerS before 0.3.10 allows remote attackers to cause a denial of service (daemon crash) via a crafted type_offset value in a TCP packet to port 30003.	trousers	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413552
8653	CVE-2012-0583	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.60 and earlier, and 5.5.19 and earlier, allows remote authenticated users to affect availability, related to MyISAM.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349747
8654	CVE-2012-0578	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402375
8655	CVE-2012-0574	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier, and 5.5.28 and earlier, allows remote authenticated users to affect availability via unknown vectors.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402366
8656	CVE-2012-0572	Medium		Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00402344
8657	CVE-2012-0553	High		Buffer overflow in yaSSL, as used in MySQL 5.1.x before 5.1.68 and 5.5.x before 5.5.28, has unspecified impact and attack vectors, a different vulnerability than CVE-2013-1492.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413551
8658	CVE-2012-0540	Medium		Unspecified vulnerability in Oracle MySQL Server 5.1.62 and earlier and 5.5.23 and earlier allows remote authenticated users to affect availability, related to GIS Extension.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366806
8659	CVE-2012-0492	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0485.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330864
8660	CVE-2012-0490	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect availability via unknown vectors.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330849
8661	CVE-2012-0485	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0492.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330848
8662	CVE-2012-0484	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect confidentiality via unknown vectors.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330847
8663	CVE-2012-0441	Medium		The ASN.1 decoder in the QuickDER decoder in Mozilla Network Security Services (NSS) before 3.13.4, as used in Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10, allows remote attackers to cause a denial of service (application crash) via a zero-length item, as demonstrated by (1) a zero-length basic constraint or (2) a zero-length field in an OCSP response.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411209

	A	B	C	D	E	F	G	H	I	J	K	L	M
8664	CVE-2012-0420	Medium		zypp-refresh-wrapper in SUSE Zypper before 1.3.20 and 1.6.x before 1.6.166 allows local users to create files in arbitrary directories, or possibly have unspecified other impact, via a pathname in the ZYPP_LOCKFILE_ROOT environment variable.	zypper	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6742
8665	CVE-2012-0390	Medium		The DTLS implementation in GnuTLS 3.0.10 and earlier executes certain error-handling code only if there is a specific relationship between a padding length and the ciphertext size, which makes it easier for remote attackers to recover partial plaintext via a timing side-channel attack, a related issue to CVE-2011-4108.	GnuTLS	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00328000
8666	CVE-2012-0260	Medium		The JPEGWarningHandler function in coders/jpeg.c in ImageMagick before 6.7.6-3 allows remote attackers to cause a denial of service (memory consumption) via a JPEG image with a crafted sequence of restart markers.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355880
8667	CVE-2012-0259	Medium		The GetEXIFProperty function in magick/property.c in ImageMagick before 6.7.6-3 allows remote attackers to cause a denial of service (crash) via a zero value in the component count of an EXIF XResolution tag in a JPEG file, which triggers an out-of-bounds read.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355872
8668	CVE-2012-0256	Medium		Apache Traffic Server 2.0.x and 3.0.x before 3.0.4 and 3.1.x before 3.1.3 does not properly allocate heap memory, which allows remote attackers to cause a denial of service (daemon crash) via a long HTTP Host header.	apache traffic server	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00343364
8669	CVE-2012-0255	Medium		The BGP implementation in bgpd in Quagga before 0.99.20.1 does not properly use message buffers for OPEN messages, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a message associated with a malformed Four-octet AS Number Capability (aka AS4 capability).	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00345311
8670	CVE-2012-0250	Low		Buffer overflow in the OSPFv2 implementation in ospfd in Quagga before 0.99.20.1 allows remote attackers to cause a denial of service (daemon crash) via a Link State Update (aka LS Update) packet containing a network-LSA link-state advertisement for which the data-structure length is smaller than the value in the Length header field.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00345313
8671	CVE-2012-0249	Low		Buffer overflow in the ospf_ls_upd_list_lsa function in ospf_packet.c in the OSPFv2 implementation in ospfd in Quagga before 0.99.20.1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a Link State Update (aka LS Update) packet that is smaller than the length specified in its header.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00345310
8672	CVE-2012-0248	Medium		ImageMagick 6.7.5-7 and earlier allows remote attackers to cause a denial of service (infinite loop and hang) via a crafted image whose IFD contains IOP tags that all reference the beginning of the IDF.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355873
8673	CVE-2012-0247	High		ImageMagick 6.7.5-7 and earlier allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via crafted offset and count values in the ResolutionUnit tag in the EXIF IFD0 of an image.	imagemagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355882
8674	CVE-2012-0219	Medium		Heap-based buffer overflow in the xioscan_readline function in xio-readline.c in socat 1.4.0.0 through 1.7.2.0 and 2.0.0-b1 through 2.0.0-b4 allows local users to execute arbitrary code via the READLINE address.	socat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00411207
8675	CVE-2012-0216	Medium		The default configuration of the apache2 package in Debian GNU/Linux squeeze before 2.2.16-6+squeeze7, wheezy before 2.2.22-4, and sid before 2.2.22-4, when mod_php or mod_rivet is used, provides example scripts under the doc/ URI, which might allow local users to conduct cross-site scripting (XSS) attacks, gain privileges, or obtain sensitive information via vectors involving localhost HTTP requests to the Apache HTTP Server.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347664
8676	CVE-2012-0213	Medium		The UnhandledDataStructure function in hwpf/model/UnhandledDataStructure.java in Apache POI 3.8 and earlier allows remote attackers to cause a denial of service (OutOfMemoryError exception and possibly JVM destabilization) via a crafted length value in a Channel Definition Format (CDF) or Compound File Binary Format (CFBF) document.	Apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00370228
8677	CVE-2012-0207	High		The igmp_heard_query function in net/ipv4/igmp.c in the Linux kernel before 3.2.1 allows remote attackers to cause a denial of service (divide-by-zero error and panic) via IGMP packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353064
8678	CVE-2012-0120	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0485, and CVE-2012-0492.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330846
8679	CVE-2012-0119	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330845
8680	CVE-2012-0118	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and availability via unknown vectors, a different vulnerability than CVE-2012-0113.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330844
8681	CVE-2012-0116	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and integrity via unknown vectors.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330843

	A	B	C	D	E	F	G	H	I	J	K	L	M
8682	CVE-2012-0115	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330842
8683	CVE-2012-0114	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows local users to affect confidentiality and integrity via unknown vectors.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330841
8684	CVE-2012-0113	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and availability via unknown vectors, a different vulnerability than CVE-2012-0118.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330840
8685	CVE-2012-0112	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330839
8686	CVE-2012-0102	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0087 and CVE-2012-0101.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330838
8687	CVE-2012-0101	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0087 and CVE-2012-0102.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330837
8688	CVE-2012-0087	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0101 and CVE-2012-0102.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330824
8689	CVE-2012-0075	Low		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect integrity via unknown vectors.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330822
8690	CVE-2012-0064	Medium		xkeyboard-config before 2.5 in X.Org before 7.6 enables certain XKB debugging functions by default, which allows physically proximate attackers to bypass an X screen lock via keyboard combinations that break the input grab.	x.org	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6753
8691	CVE-2012-0061	Medium		The headerLoad function in lib/header.c in RPM before 4.9.1.3 does not properly validate region tags, which allows user-assisted remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large region size in a package header.	rpm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355879
8692	CVE-2012-0060	Medium		RPM before 4.9.1.3 does not properly validate region tags, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an invalid region tag in a package header to the (1) headerLoad, (2) rpmReadSignature, or (3) headerVerify function.	rpm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355883
8693	CVE-2012-0058	Medium		The kiocb_batch_free function in fs/aio.c in the Linux kernel before 3.2.2 allows local users to cause a denial of service (OOPS) via vectors that trigger incorrect iocb management.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353065
8694	CVE-2012-0057	Medium		PHP before 5.3.9 has improper libxslt security settings, which allows remote attackers to create arbitrary files via a crafted XSLT stylesheet that uses the libxslt output extension.	php.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334434
8695	CVE-2012-0056	Medium		The mem_write function in Linux kernel 2.6.39 and other versions, when ASLR is disabled, does not properly check permissions when writing to /proc/<pid>/mem, which allows local users to gain privileges by modifying process memory, as demonstrated by Mempodipper.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332171
8696	CVE-2012-0053	Medium		protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332159
8697	CVE-2012-0050	Medium		OpenSSL 0.9.8s and 1.0.0f does not properly support DTLS applications, which allows remote attackers to cause a denial of service via unspecified vectors. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-4108.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330866
8698	CVE-2012-0047	Medium		Cross-site scripting (XSS) vulnerability in Apache Wicket 1.4.x before 1.4.20 allows remote attackers to inject arbitrary web script or HTML via the wicket:pageMapName parameter.	apache wicket	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00343365
8699	CVE-2012-0045	Medium		The em_syscall function in arch/x86/kvm/emulate.c in the KVM implementation in the Linux kernel before 3.2.14 does not properly handle the 0f05 (aka syscall) opcode, which allows guest OS users to cause a denial of service (guest OS crash) via a crafted application, as demonstrated by an NASM file.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362911
8700	CVE-2012-0044	High		Integer overflow in the drm_mode_dirtyfb_ioctl function in drivers/gpu/drm/drm_crtc.c in the Direct Rendering Manager (DRM) subsystem in the Linux kernel before 3.1.5 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted ioctl call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353077
8701	CVE-2012-0038	Medium		Integer overflow in the xfs_acl_from_disk function in fs/xfs/xfs_acl.c in the Linux kernel before 3.1.9 allows local users to cause a denial of service (panic) via a filesystem with a malformed ACL, leading to a heap-based buffer overflow.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353071

	A	B	C	D	E	F	G	H	I	J	K	L	M
8702	CVE-2012-0037	Medium		Redland Raptor (aka libraptor) before 2.0.7, as used by OpenOffice 3.3 and 3.4 Beta, LibreOffice before 3.4.6 and 3.5.x before 3.5.1, and other products, allows user-assisted remote attackers to read arbitrary files via a crafted XML external entity (XXE) declaration and reference in an RDF document.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359320
8703	CVE-2012-0036	High		curl and libcurl 7.2x before 7.24.0 do not properly consider special characters during extraction of a pathname from a URL, which allows remote attackers to conduct data-injection attacks via a crafted URL, as demonstrated by a CRLF injection attack on the (1) IMAP, (2) POP3, or (3) SMTP protocol.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00347682
8704	CVE-2012-0031	Medium		scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330583
8705	CVE-2012-0029	High		Heap-based buffer overflow in the process_tx_desc function in the e1000 emulation (hw/e1000.c) in qemu-kvm 0.12, and possibly other versions, allows guest OS users to cause a denial of service (QEMU crash) and possibly execute arbitrary code via crafted legacy mode packets.	qemu-kvm.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332173
8706	CVE-2012-0028	High		The robust futex implementation in the Linux kernel before 2.6.28 does not properly handle processes that make exec system calls, which allows local users to cause a denial of service or possibly gain privileges by writing to a memory location in a child process.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359304
8707	CVE-2012-0027	Medium		The GOST ENGINE in OpenSSL before 1.0.0f does not properly handle invalid parameters for the GOST block cipher, which allows remote attackers to cause a denial of service (daemon crash) via crafted data from a TLS client.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00327999
8708	CVE-2012-0021	Low		The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server 2.2.17 through 2.2.21, when a threaded MPM is used, does not properly handle a %{}C format string, which allows remote attackers to cause a denial of service (daemon crash) via a cookie that lacks both a name and a value.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332158
8709	CVE-2011-5327			In the Linux kernel before 3.1, an off by one in the drivers/target/loopback/tcm_loop.c tcm_loop_make_naa_tpg() function could result in at least memory corruption.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4549
8710	CVE-2011-5326	MEDIUM		imlib2 before 1.4.9 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) by drawing an 2x1 ellipse.	imlib2	Unchanged	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-592
8711	CVE-2011-5325			Directory traversal vulnerability in the BusyBox implementation of tar before 1.22.0 v5 allows remote attackers to point to files outside the current working directory via a symlink.	busybox	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-4949
8712	CVE-2011-5321	Medium		The tty_open function in drivers/tty/tty_io.c in the Linux kernel before 3.1.1 mishandles a driver-lookup failure, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via crafted access to a device file under the /dev/pts directory.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-612
8713	CVE-2011-5320			scanf and related functions in glibc before 2.15 allow local users to cause a denial of service (segmentation fault) via a large string of 0s.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5714
8714	CVE-2011-5244	Medium		Multiple off-by-one errors in the (1) token and (2) linetoken functions in backend/dvi/mdvi-lib/afmparse.c in t1lib, as used in teTeX 3.0.x, GNOME evince, and possibly other products, allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a DVI file containing a crafted Adobe Font Metrics (AFM) file, different vulnerabilities than CVE-2010-2642 and CVE-2011-0433.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392009
8715	CVE-2011-5222	High		SQL injection vulnerability in rub2_w.php in PHP Flirt-Projekt 4.8 and possibly earlier allows remote attackers to execute arbitrary SQL commands via the rub parameter.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386299
8716	CVE-2011-5220	Medium		Cross-site scripting (XSS) vulnerability in templates/default/Admin/Login.html in PHP-SCMS 1.6.8 and earlier allows remote attackers to inject arbitrary web script or HTML via the lang parameter to index.php.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386306
8717	CVE-2011-5095	Medium		The Diffie-Hellman key-exchange implementation in OpenSSL 0.9.8, when FIPS mode is enabled, does not properly validate a public parameter, which makes it easier for man-in-the-middle attackers to obtain the shared secret key by modifying network traffic, a related issue to CVE-2011-1923.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359356
8718	CVE-2011-5000	Low		The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00345312
8719	CVE-2011-4971	Medium		Multiple integer signedness errors in the (1) process_bin_sasl_auth, (2) process_bin_complete_sasl_auth, (3) process_bin_update, and (4) process_bin_append_prepend functions in Memcached 1.4.5 and earlier allow remote attackers to cause a denial of service (crash) via a large body length value in a packet.	memcached	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448743
8720	CVE-2011-4966	Medium		modules/rlm_unix/rlm_unix.c in FreeRADIUS before 2.2.0, when unix mode is enabled for user authentication, does not properly check the password expiration in /etc/shadow, which allows remote authenticated users to authenticate using an expired password.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413585

	A	B	C	D	E	F	G	H	I	J	K	L	M
8721	CVE-2011-4944	Low		Python 2.6 through 3.2 creates ~/.pypirc with world-readable permissions before changing them after data has been written, which introduces a race condition that allows local users to obtain a username and password by reading this file.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374009
8722	CVE-2011-4940	Low		The list_directory function in Lib/SimpleHTTPServer.py in SimpleHTTPServer in Python before 2.5.6c1, 2.6.x before 2.6.7 rc2, and 2.7.x before 2.7.2 does not place a charset parameter in the Content-Type HTTP header, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer 7 via UTF-7 encoding.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359357
8723	CVE-2011-4914	Medium		The ROSE protocol implementation in the Linux kernel before 2.6.39 does not verify that certain data-length values are consistent with the amount of data sent, which might allow remote attackers to obtain sensitive information from kernel memory or cause a denial of service (out-of-bounds read) via crafted data to a ROSE socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359350
8724	CVE-2011-4913	High		The rose_parse_ccitt function in net/rose/rose_subr.c in the Linux kernel before 2.6.39 does not validate the FAC_CCITT_DEST_NSAP and FAC_CCITT_SRC_NSAP fields, which allows remote attackers to (1) cause a denial of service (integer underflow, heap memory corruption, and panic) via a small length value in data sent to a ROSE socket, or (2) conduct stack-based buffer overflow attacks via a large length value in data sent to a ROSE socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359317
8725	CVE-2011-4885	Medium		PHP before 5.3.9 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00328001
8726	CVE-2011-4868	Medium		The logging functionality in dhcpd in ISC DHCP before 4.2.3-P2, when using Dynamic DNS (DDNS) and issuing IPv6 addresses, does not properly handle the DHCPv6 lease structure, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via crafted packets related to a lease-status update.	isc dhcp.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330584
8727	CVE-2011-4862	High		Buffer overflow in libtelnet/encrypt.c in telnetd in FreeBSD 7.3 through 9.0, MIT Kerberos Version 5 Applications (aka krb5-appl) 1.0.2 and earlier, and Heimdal 1.5.1 and earlier allows remote attackers to execute arbitrary code via a long encryption key, as exploited in the wild in December 2011.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00328006
8728	CVE-2011-4718	Medium		Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00430967
8729	CVE-2011-4622	Medium		The create_pit_timer function in arch/x86/kvm/i8254.c in KVM 83, and possibly other versions, does not properly handle when Programmable Interval Timer (PIT) interrupt requests (IRQs) when a virtual interrupt controller (irqchip) is not available, which allows local users to cause a denial of service (NULL pointer dereference) by starting a timer.	kvm.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332172
8730	CVE-2011-4621	Medium		The Linux kernel before 2.6.37 does not properly implement a certain clock-update optimization, which allows local users to cause a denial of service (system hang) via an application that executes code in a loop.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353078
8731	CVE-2011-4619	Medium		The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly handle handshake restarts, which allows remote attackers to cause a denial of service via unspecified vectors.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00327998
8732	CVE-2011-4613	Medium		The X.Org X wrapper (xserver-wrapper.c) in Debian GNU/Linux and Ubuntu Linux does not properly verify the TTY of a user who is starting X, which allows local users to bypass intended access restrictions by associating stdin with a file that is misinterpreted as the console TTY.	x.org	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6774
8733	CVE-2011-4611	Medium		Integer overflow in the perf_event_interrupt function in arch/powerpc/kernel/perf_event.c in the Linux kernel before 2.6.39 on powerpc platforms allows local users to cause a denial of service (unhandled performance monitor exception) via vectors that trigger certain outcomes of performance events.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353052
8734	CVE-2011-4609	Medium		The svc_run function in the RPC implementation in glibc before 2.15 allows remote attackers to cause a denial of service (CPU consumption) via a large number of RPC connections.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417549
8735	CVE-2011-4604	Medium		The bat_socket_read function in net/batman-adv/icmp_socket.c in the Linux kernel before 3.3 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted batman-adv ICMP packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421915
8736	CVE-2011-4600	Medium		The networkReloadIptablesRules function in network/bridge_driver.c in libvirt before 0.9.9 does not properly handle firewall rules on bridge networks when libvirtd is restarted, which might allow remote attackers to bypass intended access restrictions via a (1) DNS or (2) DHCP query.	libvirt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-479
8737	CVE-2011-4594	Medium		The __sys_sendmsg function in net/socket.c in the Linux kernel before 3.1 allows local users to cause a denial of service (system crash) via crafted use of the sendmmsg system call, leading to an incorrect pointer dereference.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353045
8738	CVE-2011-4577	Medium		OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00327997

	A	B	C	D	E	F	G	H	I	J	K	L	M
8739	CVE-2011-4576	Medium		The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00327996
8740	CVE-2011-4539	Medium		dhcpd in ISC DHCP 4.x before 4.2.3-P1 and 4.1-ESV before 4.1-ESV-R4 does not properly handle regular expressions in dhcpd.conf, which allows remote attackers to cause a denial of service (daemon crash) via a crafted request packet.	isc dhcp.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00322935
8741	CVE-2011-4415	Low		The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the len += statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00318513
8742	CVE-2011-4408	Medium		The Single Sign On Client (ubuntu-sso-client) for Ubuntu 11.04 and 11.10 does not properly validate SSL certificates when using HTTPS, which allows remote attackers to spoof a server and modify or read sensitive data via a man-in-the-middle (MITM) attack.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359308
8743	CVE-2011-4363	Low		ProcessTable.pm in the Proc::ProcessTable module 0.45 for Perl, when TTY information caching is enabled, allows local users to overwrite arbitrary files via a symlink attack on /tmp/TTYDEVS.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382755
8744	CVE-2011-4355	Medium		GNU Project Debugger (GDB) before 7.5, when .debug_gdb_scripts is defined, automatically loads certain files from the current working directory, which allows local users to gain privileges via crafted files such as Python scripts.	gdb	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408760
8745	CVE-2011-4354	Medium		crypto/bn/bn_nist.c in OpenSSL before 0.9.8h on 32-bit platforms, as used in stunnel and other products, in certain circumstances involving ECDH or ECDHE cipher suites, uses an incorrect modular reduction algorithm in its implementation of the P-256 and P-384 NIST elliptic curves, which allows remote attackers to obtain the private key of a TLS server via multiple handshake attempts.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332154
8746	CVE-2011-4351	High		Buffer overflow in FFmpeg before 0.5.6, 0.6.x before 0.6.4, 0.7.x before 0.7.8, and 0.8.x before 0.8.8 allows remote attackers to execute arbitrary code via unspecified vectors.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448738
8747	CVE-2011-4348	High		Race condition in the sctp_rcv function in net/sctp/input.c in the Linux kernel before 2.6.29 allows remote attackers to cause a denial of service (system hang) via SCTP packets. NOTE: in some environments, this issue exists because of an incomplete fix for CVE-2011-2482.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421914
8748	CVE-2011-4347	MEDIUM		It was found that kvm_vm_ioctl_assign_device function did not check if the user requesting assignment was privileged or not. Together with /dev/kvm being 666, unprivileged user could assign unused pci devices, or even devices that were in use and whose resources were not properly claimed by the respective drivers. Please note that privileged access was still needed to re-program the device to for example issue DMA requests. This is typically achieved by touching files on sysfs filesystem. These files are usually not accessible to unprivileged users. As a result, local user could use this flaw to crash the system. Reference: http://thread.gmane.org/gmane.comp.emulators.kvm.devel/82043	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00319335
8749	CVE-2011-4339	Low		ipmievd (aka the IPMI event daemon) in OpenIPMI, as used in the ipmitool package 1.8.11 in Red Hat Enterprise Linux (RHEL) 6, uses 0666 permissions for its ipmievd.pid PID file, which allows local users to kill arbitrary processes by writing to this file.	openipmi	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325457
8750	CVE-2011-4330	HIGH		On a corrupted file system the ->len field could be wrong leading to a buffer overflow. https://lkml.org/lkml/2011/11/9/303 Upstream commit: http://git.kernel.org/linus/bc5b8a9003132ae44559edd63a1623	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00319163
8751	CVE-2011-4328	Medium		plugin/npapi/plugin.cpp in Gnash before 0.8.10 uses weak permissions (word readable) for cookie files with predictable names in /tmp, which allows local users to obtain sensitive information.	gnu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359302
8752	CVE-2011-4327	LOW		A security flaw was found in the way ssh-keysign, a ssh helper program for host based authentication, attempted to retrieve enough entropy information on configurations that lacked a built-in entropy pool in OpenSSL (a ssh-rand-helper program would be executed to retrieve the entropy from the system environment). A local attacker could use this flaw to obtain unauthorized access to host keys via ptrace(2) process trace attached to the 'ssh-rand-helper' program.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00319164
8753	CVE-2011-4326	HIGH		A bug was found in the way headroom check was performed in udp6_ufo_fragment() function. A remote attacker could use this flaw to crash the system. Upstream patch: a9cf73ea7ff78f52662c8658d93c226effbbedde	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00319166
8754	CVE-2011-4325	Medium		The NFS implementation in Linux kernel before 2.6.31-rc6 calls certain functions without properly initializing certain data, which allows local users to cause a denial of service (NULL pointer dereference and O_DIRECT oops), as demonstrated using diotest4 from LTP.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332165
8755	CVE-2011-4324	MEDIUM		It is possible to trigger the BUG() in fs/nfs/nfs4xdr.c on a NFSv4 mount. http://git.kernel.org/linus/dc0b027dfadfcb8a5504f7d8052754bf8d501ab9.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00319130

	A	B	C	D	E	F	G	H	I	J	K	L	M
8756	CVE-2011-4317	Medium		The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00322939
8757	CVE-2011-4313	Medium		query.c in ISC BIND 9.0.x through 9.6.x, 9.4-ESV through 9.4-ESV-R5, 9.6-ESV through 9.6-ESV-R5, 9.7.0 through 9.7.4, 9.8.0 through 9.8.1, and 9.9.0a1 through 9.9.0b1 allows remote attackers to cause a denial of service (assertion failure and named exit) via unknown vectors related to recursive DNS queries, error logging, and the caching of an invalid record by the resolver.	isc bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00319168
8758	CVE-2011-4280	Medium		Cross-site scripting (XSS) vulnerability in the Spike PHPCoverage (aka spikephpcoverage) library, as used in Moodle 2.0.x before 2.0.2 and other products, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366780
8759	CVE-2011-4190			The kdump implementation is missing the host key verification in the kdump and mkdumprd OpenSSH integration of kdump prior to version 2012-01-20. This is similar to CVE-2011-3588, but different in that the kdump implementation is specific to SUSE. A remote malicious kdump server could use this flaw to impersonate the correct kdump server to obtain security sensitive information (kdump core files).	kexec	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4122
8760	CVE-2011-4151	High		The krb5_db2_lockout_audit function in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.8 through 1.8.4, when the db2 (aka Berkeley DB) back end is used, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via unspecified vectors, a different vulnerability than CVE-2011-1528.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314629
8761	CVE-2011-4132	Low		The cleanup_journal_tail function in the Journaling Block Device (JBD) functionality in the Linux kernel 2.6 allows local users to cause a denial of service (assertion error and kernel oops) via an ext3 or ext4 image with an invalid log first block value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332164
8762	CVE-2011-4131	High		The NFSv4 implementation in the Linux kernel before 3.2.2 does not properly handle bitmap sizes in GETACL replies, which allows remote NFS servers to cause a denial of service (OOPS) by sending an excessive number of bitmap words.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353080
8763	CVE-2011-4128	Medium		Buffer overflow in the gnutls_session_get_data function in lib/gnutls_session.c in GnuTLS 2.12.x before 2.12.14 and 3.x before 3.0.7, when used on a client that performs nonstandard session resumption, allows remote TLS servers to cause a denial of service (application crash) via a large SessionTicket.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00322936
8764	CVE-2011-4127	Medium		The Linux kernel before 3.2.2 does not properly restrict SG_IO ioctl calls, which allows local users to bypass intended restrictions on disk read and write operations by sending a SCSI command to (1) a partition block device or (2) an LVM volume.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362909
8765	CVE-2011-4112	MEDIUM		running the bridge over vlan testing,I got a kernel panic at dev_queue_xmit+0x35/0x4d0 http://git.kernel.org/linus/550fd08c2cebad61c548def135f67aba284c6162 http://git.kernel.org/linus/d8873315065f1f527c7c380402cf59b1e1d0ae36	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00319165
8766	CVE-2011-4111	Medium		Buffer overflow in the ccid_card_vscard_handle_message function in hw/ccid-card-passthru.c in QEMU before 0.15.2 and 1.x before 1.0-rc4 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted VSC_ATR message.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6869
8767	CVE-2011-4110	LOW		A flaw was found in the way Linux kernel handled user-defined key types. An unprivileged local user could use this flaw to crash the system. Reference:https://lkml.org/lkml/2011/11/15/363	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00319143
8768	CVE-2011-4109	High		Double free vulnerability in OpenSSL 0.9.8 before 0.9.8s, when X509_V_FLAG_POLICY_CHECK is enabled, allows remote attackers to have an unspecified impact by triggering failure of a policy check.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00327992
8769	CVE-2011-4108	Medium		The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00327991
8770	CVE-2011-4107	Medium		The simplexml_load_string function in the XML import plug-in (libraries/import/xml.php) in phpMyAdmin 3.4.x before 3.4.7.1 and 3.3.x before 3.3.10.5 allows remote authenticated users to read arbitrary files via XML data containing external entity references, aka an XML external entity (XXE) injection attack.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325584
8771	CVE-2011-4099	Medium		The capsh program in libcap before 2.22 does not change the current working directory when the --chroot option is specified, which allows local users to bypass the chroot restrictions via unspecified vectors.	libcap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6752
8772	CVE-2011-4098	Low		The fallocate implementation in the GFS2 filesystem in the Linux kernel before 3.2 relies on the page cache, which might allow local users to cause a denial of service by preallocating blocks in certain situations involving insufficient memory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421921
8773	CVE-2011-4097	Medium		Integer overflow in the oom_badness function in mm/oom_kill.c in the Linux kernel before 3.1.8 on 64-bit platforms allows local users to cause a denial of service (memory consumption or process termination) by using a certain large amount of memory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353074

	A	B	C	D	E	F	G	H	I	J	K	L	M
8774	CVE-2011-4089	Medium		The bzexe command in bzip2 1.0.5 and earlier generates compressed executables that do not properly handle temporary files during extraction, which allows local users to execute arbitrary code by precreating a temporary directory.	bzip2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7283
8775	CVE-2011-4087	Medium		The br_parse_ip_options function in net/bridge/br_netfilter.c in the Linux kernel before 2.6.39 does not properly initialize a certain data structure, which allows remote attackers to cause a denial of service by leveraging connectivity to a network interface that uses an Ethernet bridge device.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421931
8776	CVE-2011-4086	Medium		The journal_unmap_buffer function in fs/jbd2/transaction.c in the Linux kernel before 3.3.1 does not properly handle the _Delay and _Unwritten buffer head states, which allows local users to cause a denial of service (system crash) by leveraging the presence of an ext4 filesystem that was mounted with a journal.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362923
8777	CVE-2011-4083	Medium		The sosreport utility in the Red Hat sos package before 1.7-9 and 2.x before 2.2-17 includes (1) Certificate-based Red Hat Network private entitlement keys and the (2) private key for the entitlement in an archive of debugging information, which might allow remote attackers to obtain sensitive information by reading the archive.	sosreport	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	OVP-1706
8778	CVE-2011-4081	Medium		crypto/ghash-generic.c in the Linux kernel before 3.1 allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact by triggering a failed or missing ghash_setkey function call, followed by a (1) ghash_update function call or (2) ghash_final function call, as demonstrated by a write operation on an AF_ALG socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353060
8779	CVE-2011-4080	Medium		The sysrq_sysctl_handler function in kernel/sysctl.c in the Linux kernel before 2.6.39 does not require the CAP_SYS_ADMIN capability to modify the dmesg_restrict value, which allows local users to bypass intended access restrictions and read the kernel ring buffer by leveraging root privileges, as demonstrated by a root user in a Linux Containers (aka LXC) environment.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353050
8780	CVE-2011-4079	Medium		Off-by-one error in the UTF8StringNormalize function in OpenLDAP 2.4.26 and earlier allows remote attackers to cause a denial of service (slapd crash) via a zero-length string that triggers a heap-based buffer overflow, as demonstrated using an empty postalAddressAttribute value.	openldap.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00316315
8781	CVE-2011-4077	Medium		Buffer overflow in the xfs_readlink function in fs/xfs/xfs_vnodeops.c in XFS in the Linux kernel 2.6, when CONFIG_XFS_DEBUG is disabled, allows local users to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via an XFS image containing a symbolic link with a long pathname.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332161
8782	CVE-2011-4029	Low		The LockServer function in os/utils.c in X.Org xserver before 1.11.2 allows local users to change the permissions of arbitrary files to 444, read those files, and possibly cause a denial of service (removed execution permission) via a symlink attack on a temporary lock file.	xorg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362914
8783	CVE-2011-4028	Low		The LockServer function in os/utils.c in X.Org xserver before 1.11.2 allows local users to determine the existence of arbitrary files via a symlink attack on a temporary lock file, which is handled differently if the file exists.	xorg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362910
8784	CVE-2011-3970	Medium		libxslt, as used in Google Chrome before 17.0.963.46, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.	libxslt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00358736
8785	CVE-2011-3950	Medium		The dirac_decode_data_unit function in libavcodec/diracdec.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via a crafted value in the reference pictures number.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448749
8786	CVE-2011-3949	Medium		The dirac_unpack_idwt_params function in libavcodec/diracdec.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via crafted Dirac data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448722
8787	CVE-2011-3946	Medium		The ff_h264_decode_sei function in libavcodec/h264_sei.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via crafted Supplemental enhancement information (SEI) data, which triggers an infinite loop.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448725
8788	CVE-2011-3944	Medium		The smacker_decode_header_tree function in libavcodec/smacker.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via crafted Smacker data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448756
8789	CVE-2011-3941	High		The decode_mb function in libavcodec/error_resilience.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via vectors related to an uninitialized block index, which triggers an out-of-bound write.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448763
8790	CVE-2011-3935	Medium		The codec_get_buffer function in ffmpeg.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via vectors related to a crafted image size.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448777
8791	CVE-2011-3934	Medium		Double free vulnerability in the vp3_update_thread_context function in libavcodec/vp3.c in FFmpeg before 0.10 allows remote attackers to have an unspecified impact via crafted vp3 data.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00448719
8792	CVE-2011-3919	High		Heap-based buffer overflow in libxml2, as used in Google Chrome before 16.0.912.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00327989
8793	CVE-2011-3905	Medium		libxml2, as used in Google Chrome before 16.0.912.63, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325460

	A	B	C	D	E	F	G	H	I	J	K	L	M
8794	CVE-2011-3639	Medium		The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00322941
8795	CVE-2011-3638	Medium		fs/ext4/extents.c in the Linux kernel before 3.0 does not mark a modified extent as dirty in certain cases of extent splitting, which allows local users to cause a denial of service (system crash) via vectors involving ext4 umount and mount operations.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408773
8796	CVE-2011-3637	Medium		The m_stop function in fs/proc/task_mmu.c in the Linux kernel before 2.6.39 allows local users to cause a denial of service (OOPS) via vectors that trigger an m_start error.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353069
8797	CVE-2011-3628	Medium		Untrusted search path vulnerability in pam_motd (aka the MOTD module) in libpam-modules before 1.1.3-2ubuntu2.1 on Ubuntu 11.10, before 1.1.2-2ubuntu8.4 on Ubuntu 11.04, before 1.1.1-4ubuntu2.4 on Ubuntu 10.10, before 1.1.1-2ubuntu5.4 on Ubuntu 10.04 LTS, and before 0.99.7.1-5ubuntu6.5 on Ubuntu 8.04 LTS, when using certain configurations such as session optional pam_motd.so, allows local users to gain privileges by modifying the PATH environment variable to reference a malicious command, as demonstrated via uname.Per: http://cwe.mitre.org/data/definitions/426.html CWE-426: Untrusted Search Path	libpam-modules	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7265
8798	CVE-2011-3620	High		Apache Qpid 0.12 does not properly verify credentials during the joining of a cluster, which allows remote attackers to obtain access to the messaging functionality and job functionality of a cluster by leveraging knowledge of a cluster-username.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00349737
8799	CVE-2011-3619	Medium		The apparmor_setprocattr function in security/apparmor/lsm.c in the Linux kernel before 3.0 does not properly handle invalid parameters, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact by writing to a /proc/######/attr/current file.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421913
8800	CVE-2011-3607	Medium		Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00318514
8801	CVE-2011-3605	Medium		The process_rs function in the router advertisement daemon (radvd) before 1.8.2, when UnicastOnly is enabled, allows remote attackers to cause a denial of service (temporary service hang) via a large number of ND_ROUTER_SOLICIT requests.	radvd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6868
8802	CVE-2011-3604	High		The process_ra function in the router advertisement daemon (radvd) before 1.8.2 allows remote attackers to cause a denial of service (stack-based buffer over-read and crash) via unspecified vectors.	radvd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6861
8803	CVE-2011-3603	Medium		The router advertisement daemon (radvd) before 1.8.2 does not properly handle errors in the privsep_init function, which causes the radvd daemon to run as root and has an unspecified impact.Per http://thread.gmane.org/gmane.comp.security.oss.general/5973/focus=6015, this vulnerablity is being assigned a CVSS base metric of AV:L/AC:M/Au:N/C:P/I:P/A:P = 4.4	radvd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7428
8804	CVE-2011-3602	Medium		Directory traversal vulnerability in device-linux.c in the router advertisement daemon (radvd) before 1.8.2 allows local users to overwrite arbitrary files, and remote attackers to overwrite certain files, via a .. (dot dot) in an interface name. NOTE: this can be leveraged with a symlink to overwrite arbitrary files.	radvd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7423
8805	CVE-2011-3601	High		Buffer overflow in the process_ra function in the router advertisement daemon (radvd) before 1.8.2 allows remote attackers to execute arbitrary code or cause a denial of service (crash) via a negative value in a label_len value.	radvd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6882
8806	CVE-2011-3599	Medium		The Crypt::DSA (aka Crypt-DSA) module 1.17 and earlier for Perl, when /dev/random is absent, uses the Data::Random module, which makes it easier for remote attackers to spoof a signature, or determine the signing key of a signed message, via a brute-force attack.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314689
8807	CVE-2011-3593	Medium		A certain Red Hat patch to the vlan_hwaccel_do_receive function in net/8021q/vlan_core.c in the Linux kernel 2.6.32 on Red Hat Enterprise Linux (RHEL) 6 allows remote attackers to cause a denial of service (system crash) via priority-tagged VLAN frames.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421909
8808	CVE-2011-3592	Low		Multiple cross-site scripting (XSS) vulnerabilities in the PMA_unInlineEditRow function in js/sql.js in phpMyAdmin 3.4.x before 3.4.5 allow remote authenticated users to inject arbitrary web script or HTML via a (1) database name, (2) table name, or (3) column name that is not properly handled after an inline-editing operation.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2569
8809	CVE-2011-3591	Low		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 3.4.x before 3.4.5 allow remote authenticated users to inject arbitrary web script or HTML via a crafted row that triggers an improperly constructed confirmation message after inline-editing and save operations, related to (1) js/functions.js and (2) js/tbl_structure.js.	phpmyadmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2577

	A	B	C	D	E	F	G	H	I	J	K	L	M
8810	CVE-2011-3590	Medium		The Red Hat mkdumprd script for kexec-tools, as distributed in the kexec-tools 1.x before 1.102pre-154 and 2.x before 2.0.0-209 packages in Red Hat Enterprise Linux, includes all of root's SSH private keys within a vmcore file, which allows context-dependent attackers to obtain sensitive information by inspecting the file content.	Kexec-tools	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6867
8811	CVE-2011-3589	Medium		The Red Hat mkdumprd script for kexec-tools, as distributed in the kexec-tools 1.x before 1.102pre-154 and 2.x before 2.0.0-209 packages in Red Hat Enterprise Linux, uses world-readable permissions for vmcore files, which allows local users to obtain sensitive information by inspecting the file content, as demonstrated by a search for a root SSH key.	Kexec-tools	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6870
8812	CVE-2011-3588	Medium		The SSH configuration in the Red Hat mkdumprd script for kexec-tools, as distributed in the kexec-tools 1.x before 1.102pre-154 and 2.x before 2.0.0-209 packages in Red Hat Enterprise Linux, disables the StrictHostKeyChecking option, which allows man-in-the-middle attackers to spoof kdump servers, and obtain sensitive core information, by using an arbitrary SSH key.	Kexec-tools	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6862
8813	CVE-2011-3464	High		Off-by-one error in the png_formatted_warning function in pngerror.c in libpng 1.5.4 through 1.5.7 might allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via unspecified vectors, which trigger a stack-based buffer overflow.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366818
8814	CVE-2011-3389	Medium		The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a BEAST attack.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00348964
8815	CVE-2011-3368	Medium		The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00311483
8816	CVE-2011-3363	Medium		The setup_cifs_sb function in fs/cifs/connect.c in the Linux kernel before 2.6.39 does not properly handle DFS referrals, which allows remote CIFS servers to cause a denial of service (system crash) by placing a referral at the root of a share.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353082
8817	CVE-2011-3359	Medium		The dma_rx function in drivers/net/wireless/b43/dma.c in the Linux kernel before 2.6.39 does not properly allocate receive buffers, which allows remote attackers to cause a denial of service (system crash) via a crafted frame.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353081
8818	CVE-2011-3353	Medium		Buffer overflow in the fuse_notify_inval_entry function in fs/fuse/dev.c in the Linux kernel before 3.1 allows local users to cause a denial of service (BUG_ON and system crash) by leveraging the ability to mount a FUSE filesystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353076
8819	CVE-2011-3348	Medium		The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary error state in the backend server) via a malformed HTTP request.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00311484
8820	CVE-2011-3347	Medium		A certain Red Hat patch to the be2net implementation in the kernel package before 2.6.32-218.el6 on Red Hat Enterprise Linux (RHEL) 6, when promiscuous mode is enabled, allows remote attackers to cause a denial of service (system crash) via non-member VLAN packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421928
8821	CVE-2011-3346	Medium		Buffer overflow in hw/scsi-disk.c in the SCSI subsystem in QEMU before 0.15.2, as used by Xen, might allow local guest users with permission to access the CD-ROM to cause a denial of service (guest crash) via a crafted SAI READ CAPACITY SCSI command. NOTE: this is only a vulnerability when root has manually modified certain permissions or ACLs.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7124
8822	CVE-2011-3328	Low		The png_handle_cHRM function in pngrutil.c in libpng 1.5.4, when color-correction support is enabled, allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a malformed PNG image containing a cHRM chunk associated with a certain zero value.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332147
8823	CVE-2011-3327	High		Heap-based buffer overflow in the ecommunity_ecom2str function in bgp_ecommunity.c in bgpd in Quagga before 0.99.19 allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code by sending a crafted BGP UPDATE message over IPv4.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314609
8824	CVE-2011-3326	Medium		The ospf_flood function in ospf_flood.c in ospfd in Quagga before 0.99.19 allows remote attackers to cause a denial of service (daemon crash) via an invalid Link State Advertisement (LSA) type in an IPv4 Link State Update message.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314599
8825	CVE-2011-3325	Medium		ospf_packet.c in ospfd in Quagga before 0.99.19 allows remote attackers to cause a denial of service (daemon crash) via (1) a 0x0a type field in an IPv4 packet header or (2) a truncated IPv4 Hello packet.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314589

	A	B	C	D	E	F	G	H	I	J	K	L	M
8826	CVE-2011-3324	Medium		The ospf6_lsa_is_changed function in ospf6_lsa.c in the OSPFv3 implementation in ospf6d in Quagga before 0.99.19 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via trailing zero values in the Link State Advertisement (LSA) header list of an IPv6 Database Description message.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314579
8827	CVE-2011-3323	Medium		The OSPFv3 implementation in ospf6d in Quagga before 0.99.19 allows remote attackers to cause a denial of service (out-of-bounds memory access and daemon crash) via a Link State Update message with an invalid IPv6 prefix length.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314569
8828	CVE-2011-3268	High		Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325871
8829	CVE-2011-3267	Medium		PHP before 5.3.7 does not properly implement the error_log function, which allows context-dependent attackers to cause a denial of service (application crash) via unspecified vectors.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325873
8830	CVE-2011-3210	Medium		The ephemeral ECDH ciphersuite functionality in OpenSSL 0.9.8 through 0.9.8s and 1.0.x before 1.0.0e does not ensure thread safety during processing of handshake messages, which allows remote attackers to cause a denial of service (application crash) via out-of-order messages that violate the TLS protocol.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00311488
8831	CVE-2011-3209	Medium		The div_long_long_rem implementation in include/asm-x86/div64.h in the Linux kernel before 2.6.26 on the x86 platform allows local users to cause a denial of service (Divide Error Fault and panic) via a clock_gettime system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382764
8832	CVE-2011-3207	Medium		crypto/x509/x509_vfy.c in OpenSSL 1.0.x before 1.0.0e does not initialize certain structure members, which makes it easier for remote attackers to bypass CRL validation by using a nextUpdate value corresponding to a time in the past.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00311487
8833	CVE-2011-3194	High		Buffer overflow in the TIFF reader in gui/image/qtiffhandler.cpp in Qt 4.7.4 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the TIFFTAG_SAMPLESPERPIXEL tag in a greyscale TIFF image with multiple samples per pixel.	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359335
8834	CVE-2011-3193	High		Heap-based buffer overflow in the Lookup_MarkMarkPos function in the HarfBuzz module (harfbuzz-gpos.c), as used by Qt before 4.7.4 and Pango, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359316
8835	CVE-2011-3192	High		The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299581
8836	CVE-2011-3191	High		Integer signedness error in the CIFSFindNext function in fs/cifs/cifssmb.c in the Linux kernel before 3.1 allows remote CIFS servers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a large length value in a response to a read request for a directory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353079
8837	CVE-2011-3188	High		The (1) IPv4 and (2) IPv6 implementations in the Linux kernel before 3.1 use a modified MD4 algorithm to generate sequence numbers and Fragment Identification values, which makes it easier for remote attackers to cause a denial of service (disrupted networking) or hijack network sessions by predicting these values and sending crafted packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00331150
8838	CVE-2011-3182	Medium		PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325877
8839	CVE-2011-3181	Medium		Multiple cross-site scripting (XSS) vulnerabilities in the Tracking feature in phpMyAdmin 3.3.x before 3.3.10.4 and 3.4.x before 3.4.4 allow remote attackers to inject arbitrary web script or HTML via a (1) table name, (2) column name, or (3) index name.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325583
8840	CVE-2011-3170	Medium		The gif_read_lzw function in filter/image-gif.c in CUPS 1.4.8 and earlier does not properly handle the first code word in an LZW stream, which allows remote attackers to trigger a heap-based buffer overflow, and possibly execute arbitrary code, via a crafted stream, a different vulnerability than CVE-2011-2896.	apple cups.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299594
8841	CVE-2011-3149	Low		The _expand_arg function in the pam_env module (modules/pam_env/pam_env.c) in Linux-PAM (aka pam) before 1.1.5 does not properly handle when environment variable expansion can overflow, which allows local users to cause a denial of service (CPU consumption).	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366807

	A	B	C	D	E	F	G	H	I	J	K	L	M
8842	CVE-2011-3148	Medium		Stack-based buffer overflow in the _assemble_line function in modules/pam_env/pam_env.c in Linux-PAM (aka pam) before 1.1.5 allows local users to cause a denial of service (crash) and possibly execute arbitrary code via a long string of white spaces at the beginning of the ~/.pam_environment file.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366802
8843	CVE-2011-3146	Medium		librsvg before 2.34.1 uses the node name to identify the type of node, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference) and possibly execute arbitrary code via a SVG file with a node with the element name starting with fe, which is misidentified as a RsvgFilterPrimitive.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476 Null Pointer Dereference'	librsvg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376773
8844	CVE-2011-3048	Medium		The png_set_text_2 function in pngset.c in libpng 1.0.x before 1.0.59, 1.2.x before 1.2.49, 1.4.x before 1.4.11, and 1.5.x before 1.5.10 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted text chunk in a PNG image file, which triggers a memory allocation failure that is not properly handled, leading to a heap-based buffer overflow.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353043
8845	CVE-2011-3009	Medium		Ruby before 1.8.6-p114 does not reset the random seed upon forking, which makes it easier for context-dependent attackers to predict the values of random numbers by leveraging knowledge of the number sequence obtained in a different child process, a related issue to CVE-2003-0900.	ruby.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00294094
8846	CVE-2011-2964	Medium		foomaticrip.c in foomatic-rip in foomatic-filters in Foomatic 4.0.6 allows remote attackers to execute arbitrary code via a crafted *FoomaticRIPCommandLine field in a .ppd file, a different vulnerability than CVE-2011-2697.	foomatic.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291618
8847	CVE-2011-2942	Medium		A certain Red Hat patch to the __br_deliver function in net/bridge/br_forward.c in the Linux kernel 2.6.18 on Red Hat Enterprise Linux (RHEL) 5 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by leveraging connectivity to a network interface that uses an Ethernet bridge device.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421935
8848	CVE-2011-2939	Medium		Off-by-one error in the decode_xs function in Unicode/Unicode.xs in the Encode module before 2.44, as used in Perl before 5.15.6, might allow context-dependent attackers to cause a denial of service (memory corruption) via a crafted Unicode string, which triggers a heap-based buffer overflow.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330867
8849	CVE-2011-2928	Medium		The befs_follow_link function in fs/befs/linuxvfs.c in the Linux kernel before 3.1-rc3 does not validate the length attribute of long symlinks, which allows local users to cause a denial of service (incorrect pointer dereference and OOPS) by accessing a long symlink on a malformed Be filesystem.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299601
8850	CVE-2011-2918	Medium		The Performance Events subsystem in the Linux kernel before 3.1 does not properly handle event overflows associated with PERF_COUNT_SW_CPU_CLOCK events, which allows local users to cause a denial of service (system hang) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353058
8851	CVE-2011-2909	Medium		The do_devinfo_ioctl function in drivers/staging/comedi/comedi_fops.c in the Linux kernel before 3.1 allows local users to obtain sensitive information from kernel memory via a copy of a short string.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6883
8852	CVE-2011-2906	Medium		** DISPUTED ** Integer signedness error in the pmcraid_ioctl_passthrough function in drivers/scsi/pmcraid.c in the Linux kernel before 3.1 might allow local users to cause a denial of service (memory consumption or memory corruption) via a negative size value in an ioctl call. NOTE: this may be a vulnerability only in unusual environments that provide a privileged program for obtaining the required file descriptor.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353056
8853	CVE-2011-2905	Medium		Untrusted search path vulnerability in the perf_config function in tools/perf/util/config.c in perf, as distributed in the Linux kernel before 3.1, allows local users to overwrite arbitrary files via a crafted config file in the current working directory.Per: http://cwe.mitre.org/data/definitions/426.html 'CWE-426 Untrusted Search Path'	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408761
8854	CVE-2011-2898	Medium		net/packet/af_packet.c in the Linux kernel before 2.6.39.3 does not properly restrict user-space access to certain packet data structures associated with VLAN Tag Control Information, which allows local users to obtain potentially sensitive information via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353072
8855	CVE-2011-2896	Medium		The LZW decompressor in the LWZReadByte function in giftoppm.c in the David Koblas GIF decoder in PBMPLUS, as used in the gif_read_lzw function in filter/image-gif.c in CUPS before 1.4.7, the LZWReadByte function in plug-ins/common/file-gif-load.c in GIMP 2.6.11 and earlier, the LZWReadByte function in img/gifread.c in XPCE in SWI-Prolog 5.10.4 and earlier, and other products, does not properly handle code words that are absent from the decompression table when encountered, which allows remote attackers to trigger an infinite loop or a heap-based buffer overflow, and possibly execute arbitrary code, via a crafted compressed stream, a related issue to CVE-2006-1168 and CVE-2011-2895.	apple cups.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299595

	A	B	C	D	E	F	G	H	I	J	K	L	M
8856	CVE-2011-2895	High		The LZW decompressor in (1) the BufCompressedFill function in fontfile/decompress.c in X.Org libXfont before 1.4.4 and (2) compress/compress.c in 4.3BSD, as used in zopen.c in OpenBSD before 3.8, FreeBSD, NetBSD, FreeType 2.1.9, and other products, does not properly handle code words that are absent from the decompression table when encountered, which allows context-dependent attackers to trigger an infinite loop or a heap-based buffer overflow, and possibly execute arbitrary code, via a crafted compressed stream, a related issue to CVE-2006-1168 and CVE-2011-2896.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299596
8857	CVE-2011-2834	Medium		Double free vulnerability in libxml2, as used in Google Chrome before 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.	xmlsoft libxml2.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00316312
8858	CVE-2011-2821	High		Double free vulnerability in libxml2, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted XPath expression.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00316312
8859	CVE-2011-2766	High		The FCGI (aka Fast CGI) module 0.70 through 0.73 for Perl, as used by CGI::Fast, uses environment variable values from one request during processing of a later request, which allows remote attackers to bypass authentication via crafted HTTP headers.	perl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00311489
8860	CVE-2011-2749	High		The server in ISC DHCP 3.x and 4.x before 4.2.2, 3.1-ESV before 3.1-ESV-R3, and 4.1-ESV before 4.1-ESV-R3 allows remote attackers to cause a denial of service (daemon exit) via a crafted BOOTP packet.	isc dhcp.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00294088
8861	CVE-2011-2748	High		The server in ISC DHCP 3.x and 4.x before 4.2.2, 3.1-ESV before 3.1-ESV-R3, and 4.1-ESV before 4.1-ESV-R3 allows remote attackers to cause a denial of service (daemon exit) via a crafted DHCP packet.	isc dhcp.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00294088
8862	CVE-2011-2728	Medium		The bsd_glob function in the File::Glob module for Perl before 5.14.2 allows context-dependent attackers to cause a denial of service (crash) via a glob expression with the GLOB_ALTDIRFUNC flag, which triggers an uninitialized pointer dereference.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397027
8863	CVE-2011-2724	Low		The check_mtab function in client/mount.cifs.c in mount.cifs in smbfs in Samba 3.5.10 and earlier does not properly verify that the (1) device name and (2) mountpoint strings are composed of valid characters, which allows local users to cause a denial of service (mtab corruption) via a crafted string. NOTE: this vulnerability exists because of an incorrect fix for CVE-2010-0547.	samba.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306468
8864	CVE-2011-2723	Medium		The skb_gro_header_slow function in include/linux/netdevice.h in the Linux kernel before 2.6.39.4, when Generic Receive Offload (GRO) is enabled, resets certain fields in incorrect situations, which allows remote attackers to cause a denial of service (system crash) via crafted network traffic.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306465
8865	CVE-2011-2719	Medium		libraries/auth/swekey/swekey.auth.lib.php in phpMyAdmin 3.x before 3.3.10.3 and 3.4.x before 3.4.3.2 does not properly manage sessions associated with Swekey authentication, which allows remote attackers to modify the SESSION superglobal array, other superglobal arrays, and certain swekey.auth.lib.php local variables via a crafted query string, a related issue to CVE-2011-2505.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325581
8866	CVE-2011-2716	Medium		The DHCP client (udhcpc) in BusyBox before 1.20.0 allows remote DHCP servers to execute arbitrary commands via shell metacharacters in the (1) HOST_NAME, (2) DOMAIN_NAME, (3) NIS_DOMAIN, and (4) TFTP_SERVER_NAME host name options.	busybox	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362925
8867	CVE-2011-2709	Medium		libgssapi and libgssglue before 0.4 do not properly check privileges, which allows local users to load untrusted configuration files and execute arbitrary code via the GSSAPI_MECH_CONF environment variable, as demonstrated using mount.nfs.	libgssglue	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00413562
8868	CVE-2011-2707	Medium		The ptrace_setxregs function in arch/xtensa/kernel/ptrace.c in the Linux kernel before 3.1 does not validate user-space pointers, which allows local users to obtain sensitive information from kernel memory locations via a crafted PTRACE_SETXTREGS request.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353083
8869	CVE-2011-2705	Medium		The SecureRandom.random_bytes function in lib/securerandom.rb in Ruby before 1.8.7-p352 and 1.9.x before 1.9.2-p290 relies on PID values for initialization, which makes it easier for context-dependent attackers to predict the result string by leveraging knowledge of random strings obtained in an earlier process with the same PID.	ruby.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00294092
8870	CVE-2011-2702	Medium		Integer signedness error in Glibc before 2.13 and eglibc before 2.13, when using Supplemental Streaming SIMD Extensions 3 (SSSE3) optimization, allows context-dependent attackers to execute arbitrary code via a negative length parameter to (1) memcpy-ssse3-rep.S, (2) memcpy-ssse3.S, or (3) memset-sse2.S in sysdeps/i386/i686/multiarch/, which triggers an out-of-bounds read, as demonstrated using the memcpy function.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8646
8871	CVE-2011-2701	Medium		The ocsp_check function in rlm_eap_tls.c in FreeRADIUS 2.1.11, when OCSP is enabled, does not properly parse replies from OCSP responders, which allows remote attackers to bypass authentication by using the EAP-TLS protocol with a revoked X.509 client certificate.	freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00294090

	A	B	C	D	E	F	G	H	I	J	K	L	M
8872	CVE-2011-2700	Low		Multiple buffer overflows in the si4713_write_econtrol_string function in drivers/media/radio/si4713-i2c.c in the Linux kernel before 2.6.39.4 on the N900 platform might allow local users to cause a denial of service or have unspecified other impact via a crafted s_ext_ctrls operation with a (1) V4L2_CID_RDS_TX_PS_NAME or (2) V4L2_CID_RDS_TX_RADIO_TEXT control ID.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306466
8873	CVE-2011-2699	High		The IPv6 implementation in the Linux kernel before 3.1 does not generate Fragment Identification values separately for each destination, which makes it easier for remote attackers to cause a denial of service (disrupted networking) by predicting these values and sending crafted packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00331156
8874	CVE-2011-2696	Medium		Integer overflow in libsndfile before 1.0.25 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PARIS Audio Format (PAF) file that triggers a heap-based buffer overflow.	libsndfile.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291622
8875	CVE-2011-2695	Medium		Multiple off-by-one errors in the ext4 subsystem in the Linux kernel before 3.0-rc5 allow local users to cause a denial of service (BUG_ON and system crash) by accessing a sparse file in extent format with a write operation involving a block number corresponding to the largest possible 32-bit unsigned integer.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291627
8876	CVE-2011-2694	Low		Cross-site scripting (XSS) vulnerability in the chg_passwd function in web/swat.c in the Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.10 allows remote authenticated administrators to inject arbitrary web script or HTML via the username parameter to the passwd program (aka the user field to the Change Password page).Per: http://www.samba.org/samba/security/CVE-2011-2694 'Note that SWAT must be enabled in order for this vulnerability to be exploitable. By default, SWAT is *not* enabled on a Samba install.'	samba.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291633
8877	CVE-2011-2693	Low		The perf subsystem in the kernel package 2.6.32-122.el6.x86_64 in Red Hat Enterprise Linux (RHEL) 6 does not properly handle NMIs, which might allow local users to cause a denial of service (excessive log messages) via unspecified vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421927
8878	CVE-2011-2692	Medium		The png_handle_sCAL function in pngrutil.c in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.4 does not properly handle invalid sCAL chunks, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a crafted PNG image that triggers the reading of uninitialized memory.	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291620
8879	CVE-2011-2691	Medium		The png_err function in pngerror.c in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.4 makes a function call using a NULL pointer argument instead of an empty-string argument, which allows remote attackers to cause a denial of service (application crash) via a crafted PNG image.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291619
8880	CVE-2011-2690	Medium		Buffer overflow in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.4, when used by an application that calls the png_rgb_to_gray function but not the png_set_expand function, allows remote attackers to overwrite memory with an arbitrary amount of data, and possibly have unspecified other impact, via a crafted PNG image.	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291617
8881	CVE-2011-2689	Medium		The gfs2_fallocate function in fs/gfs2/file.c in the Linux kernel before 3.0-rc1 does not ensure that the size of a chunk allocation is a multiple of the block size, which allows local users to cause a denial of service (BUG and system crash) by arranging for all resource groups to have too little free space.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291623
8882	CVE-2011-2686	Medium		Ruby before 1.8.7-p352 does not reset the random seed upon forking, which makes it easier for context-dependent attackers to predict the values of random numbers by leveraging knowledge of the number sequence obtained in a different child process, a related issue to CVE-2003-0900. NOTE: this issue exists because of a regression during Ruby 1.8.6 development.	ruby.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00294094
8883	CVE-2011-2642	Low		Multiple cross-site scripting (XSS) vulnerabilities in the table Print view implementation in tbl_printview.php in phpMyAdmin before 3.3.10.3 and 3.4.x before 3.4.3.2 allow remote authenticated users to inject arbitrary web script or HTML via a crafted table name.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325578
8884	CVE-2011-2534	Medium		Buffer overflow in the clusterip_proc_write function in net/ipv4/netfilter/ipt_CLUSTERIP.c in the Linux kernel before 2.6.39 might allow local users to cause a denial of service or have unspecified other impact via a crafted write operation, related to string data that lacks a terminating '\0' character.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286706
8885	CVE-2011-2533	Low		The configure script in D-Bus (aka DBus) 1.2.x before 1.2.28 allows local users to overwrite arbitrary files via a symlink attack on an unspecified file in /tmp/.	dbus.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286694
8886	CVE-2011-2527	Low		The change_process_uid function in os-posix.c in Qemu 0.14.0 and earlier does not properly drop group privileges when the -runas option is used, which allows local guest users to access restricted files on the host.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359330
8887	CVE-2011-2525	High		The qdisc_notify function in net/sched/sch_api.c in the Linux kernel before 2.6.35 does not prevent tc_fill_qdisc function calls referencing builtin (aka CQ_F_BUILTIN) Qdisc structures, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a crafted call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00334430

	A	B	C	D	E	F	G	H	I	J	K	L	M
8888	CVE-2011-2524	Medium		Directory traversal vulnerability in soup-uri.c in SoupServer in libsoup before 2.35.4 allows remote attackers to read arbitrary files via a %2e%2e (encoded dot dot) in a URI.	libsoup.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299599
8889	CVE-2011-2522	Medium		Multiple cross-site request forgery (CSRF) vulnerabilities in the Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.10 allow remote attackers to hijack the authentication of administrators for requests that (1) shut down daemons, (2) start daemons, (3) add shares, (4) remove shares, (5) add printers, (6) remove printers, (7) add user accounts, or (8) remove user accounts, as demonstrated by certain start, stop, and restart parameters to the status program.	samba.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291632
8890	CVE-2011-2521	Medium		The x86_assign_hw_event function in arch/x86/kernel/cpu/perf_event.c in the Performance Events subsystem in the Linux kernel before 2.6.39 does not properly calculate counter values, which allows local users to cause a denial of service (panic) via the perf program.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353062
8891	CVE-2011-2518	Medium		The tomoyo_mount_acl function in security/tomoyo/mount.c in the Linux kernel before 2.6.39.2 calls the kern_path function with arguments taken directly from a mount system call, which allows local users to cause a denial of service (OOPS) or possibly have unspecified other impact via a NULL value for the device name.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353075
8892	CVE-2011-2517	High		Multiple buffer overflows in net/wireless/nl80211.c in the Linux kernel before 2.6.39.2 allow local users to gain privileges by leveraging the CAP_NET_ADMIN capability during scan operations with a long SSID value.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00353063
8893	CVE-2011-2512	Medium		The virtio_queue_notify in qemu-kvm 0.14.0 and earlier does not properly validate the virtqueue number, which allows guest users to cause a denial of service (guest crash) and possibly execute arbitrary code via a negative number in the Queue Notify field of the Virtio Header, which bypasses a signed comparison.	qemu-kvm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359336
8894	CVE-2011-2511	Medium		Integer overflow in libvirt before 0.9.3 allows remote authenticated users to cause a denial of service (libvirtd crash) and possibly execute arbitrary code via a crafted VirDomainGetVcpus RPC call that triggers memory corruption.	redhat libvirt.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00294091
8895	CVE-2011-2508	Medium		Directory traversal vulnerability in libraries/display_tbl.lib.php in phpMyAdmin 3.x before 3.3.10.2 and 3.4.x before 3.4.3.1, when a certain MIME transformation feature is enabled, allows remote authenticated users to include and execute arbitrary local files via a ..(dot dot) in a GLOBALS[mime_map][$meta->name] [transformation] parameter.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325575
8896	CVE-2011-2507	Medium		libraries/server_synchronize.lib.php in the Synchronize implementation in phpMyAdmin 3.x before 3.3.10.2 and 3.4.x before 3.4.3.1 does not properly quote regular expressions, which allows remote authenticated users to inject a PCRE e (aka PREG_REPLACE_EVAL) modifier, and consequently execute arbitrary PHP code, by leveraging the ability to modify the SESSION superglobal array.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325572
8897	CVE-2011-2506	High		setup/lib/ConfigGenerator.class.php in phpMyAdmin 3.x before 3.3.10.2 and 3.4.x before 3.4.3.1 does not properly restrict the presence of comment closing delimiters, which allows remote attackers to conduct static code injection attacks by leveraging the ability to modify the SESSION superglobal array.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325569
8898	CVE-2011-2505	Medium		libraries/auth/swekey/swekey.auth.lib.php in the Swekey authentication feature in phpMyAdmin 3.x before 3.3.10.2 and 3.4.x before 3.4.3.1 assigns values to arbitrary parameters referenced in the query string, which allows remote attackers to modify the SESSION superglobal array via a crafted request, related to a remote variable manipulation vulnerability.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325568
8899	CVE-2011-2501	Medium		The png_format_buffer function in pngerror.c in libpng 1.0.x before 1.0.55, 1.2.x before 1.2.45, 1.4.x before 1.4.8, and 1.5.x before 1.5.4 allows remote attackers to cause a denial of service (application crash) via a crafted PNG image that triggers an out-of-bounds read during the copying of error-message data. NOTE: this vulnerability exists because of a CVE-2004-0421 regression.	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291621
8900	CVE-2011-2500	High		The host_reliable_addrinfo function in support/export/hostname.c in nfs-utils before 1.2.4 does not properly use DNS to verify access to NFS exports, which allows remote attackers to mount filesystems by establishing crafted DNS A and PTR records.	nfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6876
8901	CVE-2011-2498			VUL-0: kernel: oom: use pte pages in OOM score	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-603
8902	CVE-2011-2497	High		Integer underflow in the l2cap_config_req function in net/bluetooth/l2cap_core.c in the Linux kernel before 3.0 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a small command-size value within the command header of a Logical Link Control and Adaptation Protocol (L2CAP) configuration request, leading to a buffer overflow.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299602
8903	CVE-2011-2496	High		Integer overflow in the vma_to_resize function in mm/mremap.c in the Linux kernel before 2.6.39 allows local users to cause a denial of service (BUG_ON and system crash) via a crafted mremap system call that expands a memory mapping.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355895
8904	CVE-2011-2495	Low		fs/proc/base.c in the Linux kernel before 2.6.39.4 does not properly restrict access to /proc/#####/io files, which allows local users to obtain sensitive I/O statistics by polling a file, as demonstrated by discovering the length of another user's password.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355885

	A	B	C	D	E	F	G	H	I	J	K	L	M
8905	CVE-2011-2494	Low		kernel/taskstats.c in the Linux kernel before 3.1 allows local users to obtain sensitive I/O statistics by sending taskstats commands to a netlink socket, as demonstrated by discovering the length of another user's password.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355871
8906	CVE-2011-2493	Low		The ext4_fill_super function in fs/ext4/super.c in the Linux kernel before 2.6.39 does not properly initialize a certain error-report data structure, which allows local users to cause a denial of service (OOPS) by attempting to mount a crafted ext4 filesystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355898
8907	CVE-2011-2492	Low		The bluetooth subsystem in the Linux kernel before 3.0-rc4 does not properly initialize certain data structures, which allows local users to obtain potentially sensitive information from kernel memory via a crafted getsockopt system call, related to (1) the l2cap_sock_getsockopt_old function in net/bluetooth/l2cap_sock.c and (2) the rfcomm_sock_getsockopt_old function in net/bluetooth/rfcomm/sock.c.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291626
8908	CVE-2011-2491	Medium		The Network Lock Manager (NLM) protocol implementation in the NFS client functionality in the Linux kernel before 3.0 allows local users to cause a denial of service (system hang) via a LOCK_UN flock system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408765
8909	CVE-2011-2485	Medium		The gdk_pixbuf__gif_image_load function in gdk-pixbuf/io-gif.c in gdk-pixbuf before 2.23.5 does not properly handle certain return values, which allows remote attackers to cause a denial of service (memory consumption) via a crafted GIF image file.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362921
8910	CVE-2011-2484	Medium		The add_del_listener function in kernel/taskstats.c in the Linux kernel 2.6.39.1 and earlier does not prevent multiple registrations of exit handlers, which allows local users to cause a denial of service (memory and CPU consumption), and bypass the OOM Killer, via a crafted application.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286702
8911	CVE-2011-2483	Medium		crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325881
8912	CVE-2011-2482	High		A certain Red Hat patch to the sctp_sock_migrate function in net/sctp/socket.c in the Linux kernel before 2.6.21, as used in Red Hat Enterprise Linux (RHEL) 5, allows remote attackers to cause a denial of service (NULL pointer dereference and OOPS) via a crafted SCTP packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421926
8913	CVE-2011-2479	Medium		The Linux kernel before 2.6.39 does not properly create transparent huge pages in response to a MAP_PRIVATE mmap system call on /dev/zero, which allows local users to cause a denial of service (system crash) via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408767
8914	CVE-2011-2473	Medium		The do_dump_data function in utils/opcontrol in OProfile 0.9.6 and earlier might allow local users to create or overwrite arbitrary files via a crafted --session-dir argument in conjunction with a symlink attack on the opd_pipe file, a different vulnerability than CVE-2011-1760.	oprofile.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00283575
8915	CVE-2011-2472	Medium		Directory traversal vulnerability in utils/opcontrol in OProfile 0.9.6 and earlier might allow local users to overwrite arbitrary files via a .. (dot dot) in the --save argument, related to the --session-dir argument, a different vulnerability than CVE-2011-1760.	oprofile.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00283578
8916	CVE-2011-2471	High		utils/opcontrol in OProfile 0.9.6 and earlier might allow local users to gain privileges via shell metacharacters in the (1) --vmlinux, (2) --session-dir, or (3) --xen argument, related to the daemonrc file and the do_save_setup and do_load_setup functions, a different vulnerability than CVE-2011-1760.	oprofile.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00283577
8917	CVE-2011-2465	Low		Unspecified vulnerability in ISC BIND 9 9.8.0, 9.8.0-P1, 9.8.0-P2, and 9.8.1b1, when recursion is enabled and the Response Policy Zone (RPZ) contains DNAME or certain CNAME records, allows remote attackers to cause a denial of service (named daemon crash) via an unspecified query.	isc bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00289212
8918	CVE-2011-2464	Medium		Unspecified vulnerability in ISC BIND 9 9.6.x before 9.6-ESV-R4-P3, 9.7.x before 9.7.3-P3, and 9.8.x before 9.8.0-P4 allows remote attackers to cause a denial of service (named daemon crash) via a crafted UPDATE request.	isc bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00289214
8919	CVE-2011-2262	Medium		Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote attackers to affect availability via unknown vectors.	MySQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00330589
8920	CVE-2011-2213	Medium		The inet_diag_bc_audit function in net/ipv4/inet_diag.c in the Linux kernel before 2.6.39.3 does not properly audit INET_DIAG bytecode, which allows local users to cause a denial of service (kernel infinite loop) via crafted INET_DIAG_REQ_BYTECODE instructions in a netlink message, as demonstrated by an INET_DIAG_BC_JMP instruction with a zero yes value, a different vulnerability than CVE-2010-3880.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299600
8921	CVE-2011-2212	HIGH		It was found that virtio subsystem in qemu-kvm did not properly validate virtqueue in and out requests from the guest. A privileged guest user could use this flaw to cause buffer overflow, causing the guest to crash (denial of service) or, possibly, resulting in the privileged guest user escalating their privileges on the host.	Qemu-kvm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00283574
8922	CVE-2011-2211	High		The osf_wait4 function in arch/alpha/kernel/osf_sys.c in the Linux kernel before 2.6.39.4 on the Alpha platform uses an incorrect pointer, which allows local users to gain privileges by writing a certain integer value to kernel memory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355869

	A	B	C	D	E	F	G	H	I	J	K	L	M
8923	CVE-2011-2210	Low		The osf_getsysinfo function in arch/alpha/kernel/osf_sys.c in the Linux kernel before 2.6.39.4 on the Alpha platform does not properly restrict the data size for GSI_GET_HWRPB operations, which allows local users to obtain sensitive information from kernel memory via a crafted call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355893
8924	CVE-2011-2209	Low		Integer signedness error in the osf_sysinfo function in arch/alpha/kernel/osf_sys.c in the Linux kernel before 2.6.39.4 on the Alpha platform allows local users to obtain sensitive information from kernel memory via a crafted call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355875
8925	CVE-2011-2208	Low		Integer signedness error in the osf_getdomainname function in arch/alpha/kernel/osf_sys.c in the Linux kernel before 2.6.39.4 on the Alpha platform allows local users to obtain sensitive information from kernel memory via a crafted call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355881
8926	CVE-2011-2203	Low		The hfs_find_init function in the Linux kernel 2.6 allows local users to cause a denial of service (NULL pointer dereference and Oops) by mounting an HFS file system with a malformed MDB extent record.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332169
8927	CVE-2011-2202	Medium		The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a file path injection vulnerability.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325885
8928	CVE-2011-2200	Medium		The _dbus_header_byteswap function in dbus-marshal-header.c in D-Bus (aka DBus) 1.2.x before 1.2.28, 1.4.x before 1.4.12, and 1.5.x before 1.5.4 does not properly handle a non-native byte order, which allows local users to cause a denial of service (connection loss), obtain potentially sensitive information, or conduct unspecified state-modification attacks via crafted messages.	dbus.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286693
8929	CVE-2011-2199	High		Buffer overflow in tftp-hpa before 5.1 allows remote attackers to cause a denial of service and possibly execute arbitrary code via the utimeout option.	tftp-hpa	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7536
8930	CVE-2011-2192	Medium		The Curl_input_negotiate function in http_negotiate.c in libcurl 7.10.6 through 7.21.6, as used in curl and other products, always performs credential delegation during GSSAPI authentication, which allows remote servers to impersonate clients via GSSAPI requests.	curl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00289215
8931	CVE-2011-2189	High		net/core/net_namespace.c in the Linux kernel 2.6.32 and earlier does not properly handle a high rate of creation and cleanup of network namespaces, which makes it easier for remote attackers to cause a denial of service (memory consumption) via requests to a daemon that requires a separate namespace per connection, as demonstrated by vsftpd.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00312649
8932	CVE-2011-2184	High		The key_replace_session_keyring function in security/keys/process_keys.c in the Linux kernel before 2.6.39.1 does not initialize a certain structure member, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a KEYCTL_SESSION_TO_PARENT argument to the keyctl function, a different vulnerability than CVE-2010-2960.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306464
8933	CVE-2011-2183	Medium		Race condition in the scan_get_next_rmap_item function in mm/ksm.c in the Linux kernel before 2.6.39.3, when Kernel SamePage Merging (KSM) is enabled, allows local users to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355870
8934	CVE-2011-2182	High		The ldm_frag_add function in fs/partitions/ldm.c in the Linux kernel before 2.6.39.1 does not properly handle memory allocation for non-initial fragments, which might allow local users to conduct buffer overflow attacks, and gain privileges or obtain sensitive information, via a crafted LDM partition table. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-1017.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355900
8935	CVE-2011-2178	Medium		The virSecurityManagerGetPrivateData function in security/security_manager.c in libvirt 0.8.8 through 0.9.1 uses the wrong argument for a sizeof call, which causes incorrect processing of security manager private data that reopens disk probing and might allow guest OS users to read arbitrary files on the host OS. NOTE: this vulnerability exists because of a CVE-2010-2238 regression.	redhat libvirt.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00294095
8936	CVE-2011-2022	Medium		The agp_generic_remove_memory function in drivers/char/agp/generic.c in the Linux kernel before 2.6.38.5 does not validate a certain start parameter, which allows local users to gain privileges or cause a denial of service (system crash) via a crafted AGPIOC_UNBIND agp_ioctl ioctl call, a different vulnerability than CVE-2011-1745.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277737
8937	CVE-2011-1951	Medium		lib/logmatcher.c in Balabit syslog-ng before 3.2.4, when the global flag is set and when using PCRE 8.12 and possibly other versions, allows remote attackers to cause a denial of service (memory consumption) via a message that does not match a regular expression.	syslog-ng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00289213
8938	CVE-2011-1945	Low		The elliptic curve cryptography (ECC) subsystem in OpenSSL 1.0.0d and earlier, when the Elliptic Curve Digital Signature Algorithm (ECDSA) is used for the ECDHE_ECDSA cipher suite, does not properly implement curves over binary fields, which makes it easier for context-dependent attackers to determine private keys via a timing attack and a lattice calculation.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281608

	A	B	C	D	E	F	G	H	I	J	K	L	M
8939	CVE-2011-1944	High		Integer overflow in xpath.c in libxml2 2.6.x through 2.6.32 and 2.7.x through 2.7.8, and libxml 1.8.16 and earlier, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted XML file that triggers a heap-based buffer overflow when adding a new namespace node, related to handling of XPath expressions.	libxml2.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291241
8940	CVE-2011-1941	Medium		Open redirect vulnerability in the redirector feature in phpMyAdmin 3.4.x before 3.4.1 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	phpmyadmin.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332156
8941	CVE-2011-1940	Medium		Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin 3.3.x before 3.3.10.1 and 3.4.x before 3.4.1 allow remote attackers to inject arbitrary web script or HTML via a crafted table name that triggers improper HTML rendering on a Tracking page, related to (1) libraries/tbl_links.inc.php and (2) tbl_tracking.php.	phpmyadmin.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332155
8942	CVE-2011-1935			pcap-linux.c in libpcap 1.1.1 before commit ea9432fabdf4b33cbc76d9437200e028f1c47c93 when snaplen is set may truncate packets, which might allow remote attackers to send arbitrary data while avoiding detection via crafted packets.	libpcap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5733
8943	CVE-2011-1928	Medium		The fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library 1.4.3 and 1.4.4, and the Apache HTTP Server 2.2.18, allows remote attackers to cause a denial of service (infinite loop) via a URI that does not match unspecified types of wildcard patterns, as demonstrated by attacks against mod_autoindex in httpd when a /*/WEB-INF/ configuration pattern is used. NOTE: this issue exists because of an incorrect fix for CVE-2011-0419.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281595
8944	CVE-2011-1927	Medium		The ip_expire function in net/ipv4/ip_fragment.c in the Linux kernel before 2.6.39 does not properly construct ICMP_TIME_EXCEEDED packets after a timeout, which allows remote attackers to cause a denial of service (invalid pointer dereference) via crafted fragmented packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355890
8945	CVE-2011-1925	Medium		nbd-server.c in Network Block Device (nbd-server) 2.9.21 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) by causing a negotiation failure, as demonstrated by specifying a name for a non-existent export.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	nbd.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281611
8946	CVE-2011-1910	Medium		Off-by-one error in named in ISC BIND 9.x before 9.7.3-P1, 9.8.x before 9.8.0-P2, 9.4-ESV before 9.4-ESV-R4-P1, and 9.6-ESV before 9.6-ESV-R4-P1 allows remote DNS servers to cause a denial of service (assertion failure and daemon exit) via a negative response containing large RRSIG RRsets.	bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281598
8947	CVE-2011-1907	Medium		ISC BIND 9.8.x before 9.8.0-P1, when Response Policy Zones (RPZ) RRset replacement is enabled, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via an RRSIG query.	isc bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277727
8948	CVE-2011-1837	Low		The lock-counter implementation in utils/mount.ecryptfs_private.c in ecryptfs-utils before 90 allows local users to overwrite arbitrary files via unspecified vectors.	ecryptfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6855
8949	CVE-2011-1836	Medium		utils/ecryptfs-recover-private in ecryptfs-utils before 90 does not establish a subdirectory with safe permissions, which might allow local users to bypass intended access restrictions via standard filesystem operations during the recovery process.	ecryptfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6859
8950	CVE-2011-1835	Medium		The encrypted private-directory setup process in utils/ecryptfs-setup-private in ecryptfs-utils before 90 does not properly ensure that the passphrase file is created, which might allow local users to bypass intended access restrictions at a certain time in the new-user creation steps.	ecryptfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6881
8951	CVE-2011-1834	Low		utils/mount.ecryptfs_private.c in ecryptfs-utils before 90 does not properly maintain the mtab file during error conditions, which allows local users to cause a denial of service (table corruption) or bypass intended unmounting restrictions via a umount system call.	ecryptfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6853
8952	CVE-2011-1833	Low		Race condition in the ecryptfs_mount function in fs/ecryptfs/main.c in the eCryptfs subsystem in the Linux kernel before 3.1 allows local users to bypass intended file permissions via a mount.ecryptfs_private mount with a mismatched uid.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00382756
8953	CVE-2011-1832	Low		utils/mount.ecryptfs_private.c in ecryptfs-utils before 90 does not properly check mountpoint permissions, which allows local users to remove directories via a umount system call.	ecryptfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6879
8954	CVE-2011-1831	Medium		utils/mount.ecryptfs_private.c in ecryptfs-utils before 90 does not properly check mountpoint permissions, which allows local users to effectively replace any directory with a new filesystem, and consequently gain privileges, via a mount system call.	ecryptfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6866
8955	CVE-2011-1783	Medium		The mod_dav_svn module for the Apache HTTP Server, as distributed in Apache Subversion 1.5.x and 1.6.x before 1.6.17, when the SVNPathAuthz short_circuit option is enabled, allows remote attackers to cause a denial of service (infinite loop and memory consumption) in opportunistic circumstances by requesting data.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281597

	A	B	C	D	E	F	G	H	I	J	K	L	M
8956	CVE-2011-1776	Medium		The is_gpt_valid function in fs/partitions/efi.c in the Linux kernel before 2.6.39 does not check the size of an Extensible Firmware Interface (EFI) GUID Partition Table (GPT) entry, which allows physically proximate attackers to cause a denial of service (heap-based buffer overflow and OOPS) or obtain sensitive information from kernel heap memory by connecting a crafted GPT storage device, a different vulnerability than CVE-2011-1577.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306461
8957	CVE-2011-1771	Medium		The cifs_close function in fs/cifs/file.c in the Linux kernel before 2.6.39 allows local users to cause a denial of service (NULL pointer dereference and BUG) or possibly have unspecified other impact by setting the O_DIRECT flag during an attempt to open a file on a CIFS filesystem.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306467
8958	CVE-2011-1770	High		Integer underflow in the dccp_parse_options function (net/dccp/options.c) in the Linux kernel before 2.6.33.14 allows remote attackers to cause a denial of service via a Datagram Congestion Control Protocol (DCCP) packet with an invalid feature options length, which triggers a buffer over-read.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286701
8959	CVE-2011-1768	Medium		The tunnels implementation in the Linux kernel before 2.6.34, when tunnel functionality is configured as a module, allows remote attackers to cause a denial of service (OOPS) by sending a packet during module loading.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355876
8960	CVE-2011-1767	Medium		net/ipv4/ip_gre.c in the Linux kernel before 2.6.34, when ip_gre is configured as a module, allows remote attackers to cause a denial of service (OOPS) by sending a packet during module loading.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355868
8961	CVE-2011-1760	High		utils/opcontrol in OProfile 0.9.6 and earlier might allow local users to conduct eval injection attacks and gain privileges via shell metacharacters in the -e argument.	oprofile.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00283576
8962	CVE-2011-1759	Medium		Integer overflow in the sys_oabi_semtimedop function in arch/arm/kernel/sys_oabi-compat.c in the Linux kernel before 2.6.39 on the ARM platform, when CONFIG_OABI_COMPAT is enabled, allows local users to gain privileges or cause a denial of service (heap memory corruption) by providing a crafted argument and leveraging a race condition.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00355874
8963	CVE-2011-1752	Medium		The mod_dav_svn module for the Apache HTTP Server, as distributed in Apache Subversion before 1.6.17, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a request for a baselined WebDAV resource, as exploited in the wild in May 2011.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281596
8964	CVE-2011-1751	High		The pciej_write function in hw/acpi_piix4.c in the PIIX4 Power Management emulation in qemu-kvm does not check if a device is hotpluggable before unplugging the PCI-ISA bridge, which allows privileged guest users to cause a denial of service (guest crash) and possibly execute arbitrary code by sending a crafted value to the 0xae08 (PCI_EJ_BASE) I/O port, which leads to a use-after-free related to active qemu timers.	qemu-kvm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359354
8965	CVE-2011-1750	High		Multiple heap-based buffer overflows in the virtio-blk driver (hw/virtio-blk.c) in qemu-kvm 0.14.0 allow local guest users to cause a denial of service (guest crash) and possibly gain privileges via a (1) write request to the virtio_blk_handle_write function or (2) read request to the virtio_blk_handle_read function that is not properly aligned.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359313
8966	CVE-2011-1749	Low		The nfs_addmntent function in support/nfs/nfs_mntent.c in the mount.nsf tool in nfs-utils before 1.2.4 attempts to append to the /etc/mtab file without first checking whether resource limits would interfere, which allows local users to corrupt this file via a process with a small RLIMIT_FSIZE value, a related issue to CVE-2011-1089.	nfs-utils.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6860
8967	CVE-2011-1748	Medium		The raw_release function in net/can/raw.c in the Linux kernel before 2.6.39-rc6 does not properly validate a socket data structure, which allows local users to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via a crafted release operation.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277731
8968	CVE-2011-1747	Medium		The agp subsystem in the Linux kernel 2.6.38.5 and earlier does not properly restrict memory allocation by the (1) AGPIOC_RESERVE and (2) AGPIOC_ALLOCATE ioctls, which allows local users to cause a denial of service (memory consumption) by making many calls to these ioctls.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277730
8969	CVE-2011-1746	Medium		Multiple integer overflows in the (1) agp_allocate_memory and (2) agp_create_user_memory functions in drivers/char/agp/generic.c in the Linux kernel before 2.6.38.5 allow local users to trigger buffer overflows, and consequently cause a denial of service (system crash) or possibly have unspecified other impact, via vectors related to calls that specify a large number of memory pages.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277730
8970	CVE-2011-1745	Medium		Integer overflow in the agp_generic_insert_memory function in drivers/char/agp/generic.c in the Linux kernel before 2.6.38.5 allows local users to gain privileges or cause a denial of service (system crash) via a crafted AGPIOC_BIND agp_ioctl ioctl call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277737

	A	B	C	D	E	F	G	H	I	J	K	L	M
8971	CVE-2011-1678	Low		smbfs in Samba 3.5.8 and earlier attempts to use (1) mount.cifs to append to the /etc/mtab file and (2) umount.cifs to append to the /etc/mtab.tmp file without first checking whether resource limits would interfere, which allows local users to trigger corruption of the /etc/mtab file via a process with a small RLIMIT_FSIZE value, a related issue to CVE-2011-1089.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269521
8972	CVE-2011-1677	Medium		mount in util-linux 2.19 and earlier does not remove the /etc/mtab~ lock file after a failed attempt to add a mount entry, which has unspecified impact and local attack vectors.	util-linux.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269524
8973	CVE-2011-1676	Low		mount in util-linux 2.19 and earlier does not remove the /etc/mtab.tmp file after a failed attempt to add a mount entry, which allows local users to trigger corruption of the /etc/mtab file via multiple invocations.	util-linux.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269524
8974	CVE-2011-1675	Low		mount in util-linux 2.19 and earlier attempts to append to the /etc/mtab.tmp file without first checking whether resource limits would interfere, which allows local users to trigger corruption of the /etc/mtab file via a process with a small RLIMIT_FSIZE value, a related issue to CVE-2011-1089.	util-linux.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269522
8975	CVE-2011-1659	Medium		Integer overflow in posix/fnmatch.c in the GNU C Library (aka glibc or libc6) 2.13 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a long UTF8 string that is used in an fnmatch call with a crafted pattern argument, a different vulnerability than CVE-2011-1071.	glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269487
8976	CVE-2011-1658	Low		ld.so in the GNU C Library (aka glibc or libc6) 2.13 and earlier expands the $ORIGIN dynamic string token when RPATH is composed entirely of this token, which might allow local users to gain privileges by creating a hard link in an arbitrary directory to a (1) setuid or (2) setgid program with this RPATH value, and then executing the program with a crafted value for the LD_PRELOAD environment variable, a different vulnerability than CVE-2010-3847 and CVE-2011-0536. NOTE: it is not expected that any standard operating-system distribution would ship an applicable setuid or setgid program.	glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269484
8977	CVE-2011-1598	Medium		The bcm_release function in net/can/bcm.c in the Linux kernel before 2.6.39-rc6 does not properly validate a socket data structure, which allows local users to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via a crafted release operation.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277734
8978	CVE-2011-1593	Medium		Multiple integer overflows in the next_pidmap function in kernel/pid.c in the Linux kernel before 2.6.38.4 allow local users to cause a denial of service (system crash) via a crafted (1) getdents or (2) readdir system call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277745
8979	CVE-2011-1585	Low		The cifs_find_smb_ses function in fs/cifs/connect.c in the Linux kernel before 2.6.36 does not properly determine the associations between users and sessions, which allows local users to bypass CIFS share authentication by leveraging a mount of a share by a different user.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421918
8980	CVE-2011-1581	Medium		The bond_select_queue function in drivers/net/bonding/bond_main.c in the Linux kernel before 2.6.39, when a network device with a large number of receive queues is installed but the default tx_queues setting is used, does not properly restrict queue indexes, which allows remote attackers to cause a denial of service (BUG and system crash) or possibly have unspecified other impact by sending network traffic.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281607
8981	CVE-2011-1577	Medium		Heap-based buffer overflow in the is_gpt_valid function in fs/partitions/efi.c in the Linux kernel 2.6.38 and earlier allows physically proximate attackers to cause a denial of service (OOPS) or possibly have unspecified other impact via a crafted size of the EFI GUID partition-table header on removable media.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277746
8982	CVE-2011-1573	MEDIUM		When calculating the INIT/INIT-ACK chunk length, we should not only account the length of parameters, but also the parameters zero padding length, such as AUTH HMACS parameter and CHUNKS parameter. Without the parameters zero padding length we may get following oops.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00311246
8983	CVE-2011-1550	Medium		The default configuration of logrotate on SUSE openSUSE Factory uses root privileges to process files in directories that permit non-root write access, which allows local users to conduct symlink and hard link attacks by leveraging logrotate's lack of support for untrusted directories, as demonstrated by directories for the (1) cobbler, (2) inn, (3) safte-monitor, and (4) uucp packages.	logrotate.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266144
8984	CVE-2011-1549	Medium		The default configuration of logrotate on Gentoo Linux uses root privileges to process files in directories that permit non-root write access, which allows local users to conduct symlink and hard link attacks by leveraging logrotate's lack of support for untrusted directories, as demonstrated by directories under /var/log/ for packages.	logrotate.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266144
8985	CVE-2011-1548	Medium		The default configuration of logrotate on Debian GNU/Linux uses root privileges to process files in directories that permit non-root write access, which allows local users to conduct symlink and hard link attacks by leveraging logrotate's lack of support for untrusted directories, as demonstrated by /var/log/postgresql/.	logrotate.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266144
8986	CVE-2011-1530	Medium		The process_tgs_req function in do_tgs_req.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.9 through 1.9.2 allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted TGS request that triggers an error other than the KRB5_KDB_NOENTRY error.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00322937

	A	B	C	D	E	F	G	H	I	J	K	L	M
8987	CVE-2011-1529	High		The lookup_lockout_policy function in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.8 through 1.8.4 and 1.9 through 1.9.1, when the db2 (aka Berkeley DB) or LDAP back end is used, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via vectors that trigger certain process_as_req errors.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314558
8988	CVE-2011-1528	High		The krb5_ldap_lockout_audit function in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.8 through 1.8.4 and 1.9 through 1.9.1, when the LDAP back end is used, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via unspecified vectors, related to the locked_check_p function.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314549
8989	CVE-2011-1527	High		The kdb_ldap plugin in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.9 through 1.9.1, when the LDAP back end is used, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a kinit operation with incorrect string case for the realm, related to the is_principal_in_realm, krb5_set_error_message, krb5_ldap_get_principal, and process_as_req functions.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314539
8990	CVE-2011-1526	Medium		ftpd.c in the GSS-API FTP daemon in MIT Kerberos Version 5 Applications (aka krb5-appl) 1.0.1 and earlier does not check the krb5_setegid return value, which allows remote authenticated users to bypass intended group access restrictions, and create, overwrite, delete, or read files, via standard FTP commands, related to missing autoconf tests in a configure script.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00289216
8991	CVE-2011-1521	Medium		The urllib and urllib2 modules in Python 2.x before 2.7.2 and 3.x before 3.2.1 process Location headers that specify redirection to file: URLs, which makes it easier for remote attackers to obtain sensitive information or cause a denial of service (resource consumption) via a crafted URL, as demonstrated by the file:///etc/passwd and file:///dev/zero URLs.	python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281609
8992	CVE-2011-1495	High		drivers/scsi/mpt2sas/mpt2sas_ctl.c in the Linux kernel 2.6.38 and earlier does not validate (1) length and (2) offset values before performing memory copy operations, which might allow local users to gain privileges, cause a denial of service (memory corruption), or obtain sensitive information from kernel memory via a crafted ioctl call, related to the _ctl_do_mpt_command and _ctl_diag_read_buffer functions.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277743
8993	CVE-2011-1494	Medium		Integer overflow in the _ctl_do_mpt_command function in drivers/scsi/mpt2sas/mpt2sas_ctl.c in the Linux kernel 2.6.38 and earlier might allow local users to gain privileges or cause a denial of service (memory corruption) via an ioctl call specifying a crafted value that triggers a heap-based buffer overflow.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277747
8994	CVE-2011-1493	High		Array index error in the rose_parse_national function in net/rose/rose_subr.c in the Linux kernel before 2.6.39 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by composing FAC_NATIONAL_DIGIS data that specifies a large number of digipeaters, and then sending this data to a ROSE socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359317
8995	CVE-2011-1487	Medium		The (1) lc, (2) lcfirst, (3) uc, and (4) ucfirst functions in Perl 5.10.x, 5.11.x, and 5.12.x through 5.12.3, and 5.13.x through 5.13.11, do not apply the taint attribute to the return value upon processing tainted input, which might allow context-dependent attackers to bypass the taint protection mechanism via a crafted string.	perl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269520
8996	CVE-2011-1486	Low		libvirtd in libvirt before 0.9.0 does not use thread-safe error reporting, which allows remote attackers to cause a denial of service (crash) by causing multiple threads to report errors at the same time.	libvirt.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281610
8997	CVE-2011-1479	Medium		Double free vulnerability in the inotify subsystem in the Linux kernel before 2.6.39 allows local users to cause a denial of service (system crash) via vectors involving failed attempts to create files. NOTE: this vulnerability exists because of an incorrect fix for CVE-2010-4250.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359329
8998	CVE-2011-1478	Medium		The napi_reuse_skb function in net/core/dev.c in the Generic Receive Offload (GRO) implementation in the Linux kernel before 2.6.38 does not reset the values of certain structure members, which might allow remote attackers to cause a denial of service (NULL pointer dereference) via a malformed VLAN frame.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00314529
8999	CVE-2011-1477	Medium		Multiple array index errors in sound/oss/opl3.c in the Linux kernel before 2.6.39 allow local users to cause a denial of service (heap memory corruption) or possibly gain privileges by leveraging write access to /dev/sequencer.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359305
9000	CVE-2011-1476	Medium		Integer underflow in the Open Sound System (OSS) subsystem in the Linux kernel before 2.6.39 on unspecified non-x86 platforms allows local users to cause a denial of service (memory corruption) by leveraging write access to /dev/sequencer.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359314
9001	CVE-2011-1473	Medium		** DISPUTED ** OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359328

	A	B	C	D	E	F	G	H	I	J	K	L	M
9002	CVE-2011-1471	Medium		Integer signedness error in zip_stream.c in the Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (CPU consumption) via a malformed archive file that triggers errors in zip_fread function calls.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325888
9003	CVE-2011-1470	Medium		The Zip extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a ziparchive stream that is not properly handled by the stream_get_contents function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325891
9004	CVE-2011-1469	Medium		Unspecified vulnerability in the Streams component in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) by accessing an ftp:// URL during use of an HTTP proxy with the FTP wrapper.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325892
9005	CVE-2011-1468	Medium		Multiple memory leaks in the OpenSSL extension in PHP before 5.3.6 might allow remote attackers to cause a denial of service (memory consumption) via (1) plaintext data to the openssl_encrypt function or (2) ciphertext data to the openssl_decrypt function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325950
9006	CVE-2011-1467	Medium		Unspecified vulnerability in the NumberFormatter::setSymbol (aka numfmt_set_symbol) function in the Intl extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument, a related issue to CVE-2010-4409.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325951
9007	CVE-2011-1466	Medium		Integer overflow in the SdnToJulian function in the Calendar extension in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (application crash) via a large integer in the first argument to the cal_from_jd function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325953
9008	CVE-2011-1464	Medium		Buffer overflow in the strval function in PHP before 5.3.6, when the precision configuration option has a large value, might allow context-dependent attackers to cause a denial of service (application crash) via a small numerical value in the argument.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325954
9009	CVE-2011-1425	Medium		xslt.c in XML Security Library (aka xmlsec) before 1.2.17, as used in WebKit and other products, when XSLT is enabled, allows remote attackers to create or overwrite arbitrary files via vectors involving the libxslt output extension and a ds:Transform element during signature verification.	xmlsec	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269526
9010	CVE-2011-1398	Medium		The sapi_header_op function in main/SAPI.c in PHP before 5.3.11 and 5.4.x before 5.4.0RC2 does not check for %0D sequences (aka carriage return characters), which allows remote attackers to bypass an HTTP response-splitting protection mechanism via a crafted URL, related to improper interaction between the PHP header function and certain browsers, as demonstrated by Internet Explorer and Google Chrome.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00376783
9011	CVE-2011-1182	Low		kernel/signal.c in the Linux kernel before 2.6.39 allows local users to spoof the uid and pid of a signal sender via a sigqueueinfo system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408764
9012	CVE-2011-1180	High		Multiple stack-based buffer overflows in the iriap_getvaluebyclass_indication function in net/irda/iriap.c in the Linux kernel before 2.6.39 allow remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging connectivity to an IrDA infrared network and sending a large integer value for a (1) name length or (2) attribute length.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00421930
9013	CVE-2011-1173	Medium		The econet_sendmsg function in net/econet/af_econet.c in the Linux kernel before 2.6.39 on the x86_64 platform allows remote attackers to obtain potentially sensitive information from kernel stack memory by reading uninitialized data in the ah field of an Acorn Universal Networking (AUN) packet.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286705
9014	CVE-2011-1172	Low		net/ipv6/netfilter/ip6_tables.c in the IPv6 implementation in the Linux kernel before 2.6.39 does not place the expected '\0' character at the end of string data in the values of certain structure members, which allows local users to obtain potentially sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability to issue a crafted request, and then reading the argument to the resulting modprobe process.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286707
9015	CVE-2011-1171	Low		net/ipv4/netfilter/ip_tables.c in the IPv4 implementation in the Linux kernel before 2.6.39 does not place the expected '\0' character at the end of string data in the values of certain structure members, which allows local users to obtain potentially sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability to issue a crafted request, and then reading the argument to the resulting modprobe process.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286703
9016	CVE-2011-1170	Low		net/ipv4/netfilter/arp_tables.c in the IPv4 implementation in the Linux kernel before 2.6.39 does not place the expected '\0' character at the end of string data in the values of certain structure members, which allows local users to obtain potentially sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability to issue a crafted request, and then reading the argument to the resulting modprobe process.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286704
9017	CVE-2011-1169	Medium		Array index error in the asihpi_hpi_ioctl function in sound/pci/asihpi/hpioctl.c in the AudioScience HPI driver in the Linux kernel before 2.6.38.1 might allow local users to cause a denial of service (memory corruption) or possibly gain privileges via a crafted adapter index value that triggers access to an invalid kernel pointer.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277744
9018	CVE-2011-1167	Medium		Heap-based buffer overflow in the thunder (aka ThunderScan) decoder in tif_thunder.c in LibTIFF 3.9.4 and earlier allows remote attackers to execute arbitrary code via crafted THUNDER_2BITDELTAS data in a .tiff file that has an unexpected BitsPerSample value.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266146

	A	B	C	D	E	F	G	H	I	J	K	L	M
9019	CVE-2011-1163	Low		The osf_partition function in fs/partitions/osf.c in the Linux kernel before 2.6.38 does not properly handle an invalid number of partitions, which might allow local users to obtain potentially sensitive information from kernel heap memory via vectors related to partition-table parsing.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269490
9020	CVE-2011-1162	Low		The tpm_read function in the Linux kernel 2.6 does not properly clear memory, which might allow local users to read the results of the previous TPM command.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00332163
9021	CVE-2011-1160	Low		The tpm_open function in drivers/char/tpm/tpm.c in the Linux kernel before 2.6.39 does not initialize a certain buffer, which allows local users to obtain potentially sensitive information from kernel memory via unspecified vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359327
9022	CVE-2011-1159	Low		acpid.c in acpid before 2.0.9 does not properly handle a situation in which a process has connected to acpid.socket but is not reading any data, which allows local users to cause a denial of service (daemon hang) via a crafted application that performs a connect system call but no read system calls.	acpid	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00311490
9023	CVE-2011-1155	Medium		The writeState function in logrotate.c in logrotate 3.7.9 and earlier might allow context-dependent attackers to cause a denial of service (rotation outage) via a (1) \n (newline) or (2) \ (backslash) character in a log filename, as demonstrated by a filename that is automatically constructed on the basis of a hostname or virtual machine name.	logrotate.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266141
9024	CVE-2011-1154	Medium		The shred_file function in logrotate.c in logrotate 3.7.9 and earlier might allow context-dependent attackers to execute arbitrary commands via shell metacharacters in a log filename, as demonstrated by a filename that is automatically constructed on the basis of a hostname or virtual machine name.	logrotate.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266139
9025	CVE-2011-1153	High		Multiple format string vulnerabilities in phar_object.c in the phar extension in PHP 5.3.5 and earlier allow context-dependent attackers to obtain sensitive information from process memory, cause a denial of service (memory corruption), or possibly execute arbitrary code via format string specifiers in an argument to a class method, leading to an incorrect zend_throw_exception_ex call.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325955
9026	CVE-2011-1148	High		Use-after-free vulnerability in the substr_replace function in PHP 5.3.6 and earlier allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by using the same variable for multiple arguments.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325957
9027	CVE-2011-1146	Medium		libvirt.c in the API in Red Hat libvirt 0.8.8 does not properly restrict operations in a read-only connection, which allows remote attackers to cause a denial of service (host OS crash) or possibly execute arbitrary code via a (1) virNodeDeviceDettach, (2) virNodeDeviceReset, (3) virDomainRevertToSnapshot, (4) virDomainSnapshotDelete, (5) virNodeDeviceReAttach, or (6) virConnectDomainXMLToNative call, a different vulnerability than CVE-2008-5086.	libvirt.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262184
9028	CVE-2011-1098	Medium		Race condition in the createOutputFile function in logrotate.c in logrotate 3.7.9 and earlier allows local users to read log data by opening a file before the intended permissions are in place.	logrotate.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266143
9029	CVE-2011-1097	Medium		rsync 3.x before 3.0.8, when certain recursion, deletion, and ownership options are used, allows remote rsync servers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via malformed data.	The PATCH for it is GPLv3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266370
9030	CVE-2011-1095	Medium		locale/programs/locale.c in locale in the GNU C Library (aka glibc or libc6) before 2.13 does not quote its output, which might allow local users to gain privileges via a crafted localization environment variable, in conjunction with a program that executes a script that uses the eval function.	glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269483
9031	CVE-2011-1093	High		The dccp_rcv_state_process function in net/dccp/input.c in the Datagram Congestion Control Protocol (DCCP) implementation in the Linux kernel before 2.6.38 does not properly handle packets for a CLOSED endpoint, which allows remote attackers to cause a denial of service (NULL pointer dereference and OOPS) by sending a DCCP-Close packet followed by a DCCP-Reset packet.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291630
9032	CVE-2011-1092	High		Integer overflow in ext/shmop/shmop.c in PHP before 5.3.6 allows context-dependent attackers to cause a denial of service (crash) and possibly read sensitive memory via a large third argument to the shmop_read function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325958
9033	CVE-2011-1090	Medium		The __nfs4_proc_set_acl function in fs/nfs/nfs4proc.c in the Linux kernel before 2.6.38 stores NFSv4 ACL data in memory that is allocated by kmalloc but not properly freed, which allows local users to cause a denial of service (panic) via a crafted attempt to set an ACL.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277736
9034	CVE-2011-1089	Low		The addmntent function in the GNU C Library (aka glibc or libc6) 2.13 and earlier does not report an error status for failed attempts to write to the /etc/mtab file, which makes it easier for local users to trigger corruption of this file, as demonstrated by writes from a process with a small RLIMIT_FSIZE value, a different vulnerability than CVE-2010-0296.	glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269482
9035	CVE-2011-1083	Medium		The epoll implementation in the Linux kernel 2.6.37.2 and earlier does not properly traverse a tree of epoll file descriptors, which allows local users to cause a denial of service (CPU consumption) via a crafted application that makes epoll_create and epoll_ctl system calls.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269518

	A	B	C	D	E	F	G	H	I	J	K	L	M
9036	CVE-2011-1082	Medium		fs/eventpoll.c in the Linux kernel before 2.6.38 places epoll file descriptors within other epoll data structures without properly checking for (1) closed loops or (2) deep chains, which allows local users to cause a denial of service (deadlock or stack memory consumption) via a crafted application that makes epoll_create and epoll_ctl system calls.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269518
9037	CVE-2011-1081	Medium		modrdn.c in slapd in OpenLDAP 2.4.x before 2.4.24 allows remote attackers to cause a denial of service (daemon crash) via a relative Distinguished Name (DN) modification request (aka MODRDN operation) that contains an empty value for the OldDN field.	openldap.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266366
9038	CVE-2011-1080	Low		The do_replace function in net/bridge/netfilter/ebtables.c in the Linux kernel before 2.6.39 does not ensure that a certain name field ends with a '\0' character, which allows local users to obtain potentially sensitive information from kernel stack memory by leveraging the CAP_NET_ADMIN capability to replace a table, and then reading a modprobe command line.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359331
9039	CVE-2011-1079	Medium		The bnep_sock_ioctl function in net/bluetooth/bnep/sock.c in the Linux kernel before 2.6.39 does not ensure that a certain device field ends with a '\0' character, which allows local users to obtain potentially sensitive information from kernel stack memory, or cause a denial of service (BUG and system crash), via a BNEPCONNADD command.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359307
9040	CVE-2011-1078	Low		The sco_sock_getsockopt_old function in net/bluetooth/sco.c in the Linux kernel before 2.6.39 does not initialize a certain structure, which allows local users to obtain potentially sensitive information from kernel stack memory via the SCO_CONNINFO option.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359325
9041	CVE-2011-1076	High		net/dns_resolver/dns_key.c in the Linux kernel before 2.6.38 allows remote DNS servers to cause a denial of service (NULL pointer dereference and OOPS) by not providing a valid response to a DNS query, as demonstrated by an erroneous grand.centrall.org query, which triggers improper handling of error data within a DNS resolver key.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00311486
9042	CVE-2011-1071	Medium		The GNU C Library (aka glibc or libc6) before 2.12.2 and Embedded GLIBC (EGLIBC) allow context-dependent attackers to execute arbitrary code or cause a denial of service (memory consumption) via a long UTF8 string that is used in an fnmatch call, aka a stack extension attack, a related issue to CVE-2010-2898, as originally reported for use of this library by Google Chrome.	glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269486
9043	CVE-2011-1044	Low		The ib_uverbs_poll_cq function in drivers/infiniband/core/uverbs_cmd.c in the Linux kernel before 2.6.37 does not initialize a certain response buffer, which allows local users to obtain potentially sensitive information from kernel memory via vectors that cause this buffer to be only partially filled, a different vulnerability than CVE-2010-4649.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258707
9044	CVE-2011-1025	Medium		bind.cpp in back-ndb in OpenLDAP 2.4.x before 2.4.24 does not require authentication for the root Distinguished Name (DN), which allows remote attackers to bypass intended access restrictions via an arbitrary password.	openldap.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266364
9045	CVE-2011-1024	Medium		chain.c in back-ldap in OpenLDAP 2.4.x before 2.4.24, when a master-slave configuration with a chain overlay and ppolicy_forward_updates (aka authentication-failure forwarding) is used, allows remote authenticated users to bypass external-program authentication by sending an invalid password to a slave server.	openldap.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266365
9046	CVE-2011-1023	Medium		The Reliable Datagram Sockets (RDS) subsystem in the Linux kernel before 2.6.38 does not properly handle congestion map updates, which allows local users to cause a denial of service (BUG_ON and system crash) via vectors involving (1) a loopback (aka loop) transmit operation or (2) an InfiniBand (aka ib) transmit operation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359301
9047	CVE-2011-1021	Low		drivers/acpi/debugfs.c in the Linux kernel before 3.0 allows local users to modify arbitrary kernel memory locations by leveraging root privileges to write to the /sys/kernel/debug/acpi/custom_method file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-4347.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359341
9048	CVE-2011-1020	Low		The proc filesystem implementation in the Linux kernel 2.6.37 and earlier does not restrict access to the /proc directory tree of a process after this process performs an exec of a setuid program, which allows local users to obtain sensitive information or cause a denial of service via open, lseek, read, and write system calls.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258697
9049	CVE-2011-1019	Low		The dev_load function in net/core/dev.c in the Linux kernel before 2.6.38 allows local users to bypass an intended CAP_SYS_MODULE capability requirement and load arbitrary modules by leveraging the CAP_NET_ADMIN capability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408766
9050	CVE-2011-1017	High		Heap-based buffer overflow in the ldm_frag_add function in fs/partitions/ldm.c in the Linux kernel 2.6.37.2 and earlier might allow local users to gain privileges or obtain sensitive information via a crafted LDM partition table.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262179
9051	CVE-2011-1016	Medium		The Radeon GPU drivers in the Linux kernel before 2.6.38-rc5 do not properly validate data related to the AA resolve registers, which allows local users to write to arbitrary memory locations associated with (1) Video RAM (aka VRAM) or (2) the Graphics Translation Table (GTT) via crafted values.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258696

	A	B	C	D	E	F	G	H	I	J	K	L	M
9052	CVE-2011-1015	Medium		The is_cgi method in CGIHTTPServer.py in the CGIHTTPServer module in Python 2.5, 2.6, and 3.0 allows remote attackers to read script source code via an HTTP GET request that lacks a / (slash) character at the beginning of the URI.	python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277751
9053	CVE-2011-1013	Medium		Integer signedness error in the drm_modeset_ctl function in (1) drivers/gpu/drm/drm_irq.c in the Direct Rendering Manager (DRM) subsystem in the Linux kernel before 2.6.38 and (2) sys/dev/pci/drm/drm_irq.c in the kernel in OpenBSD before 4.9 allows local users to trigger out-of-bounds write operations, and consequently cause a denial of service (system crash) or possibly have unspecified other impact, via a crafted num_crtcs (aka vb_num) structure member in an ioctl argument.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277748
9054	CVE-2011-1012	Medium		The ldm_parse_vmdb function in fs/partitions/ldm.c in the Linux kernel before 2.6.38-rc6-git6 does not validate the VBLK size value in the VMDB structure in an LDM partition table, which allows local users to cause a denial of service (divide-by-zero error and OOPS) via a crafted partition table.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262181
9055	CVE-2011-1011	Medium		The seunshare_mount function in sandbox/seunshare.c in seunshare in certain Red Hat packages of policycoreutils 2.0.83 and earlier in Red Hat Enterprise Linux (RHEL) 6 and earlier, and Fedora 14 and earlier, mounts a new directory on top of /tmp without assigning root ownership and the sticky bit to this new directory, which allows local users to replace or delete arbitrary /tmp files, and consequently cause a denial of service or possibly gain privileges, by running a setuid application that relies on /tmp, as demonstrated by the ksu application.	policycoreutils.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258709
9056	CVE-2011-1010	Medium		Buffer overflow in the mac_partition function in fs/partitions/mac.c in the Linux kernel before 2.6.37.2 allows local users to cause a denial of service (panic) or possibly have unspecified other impact via a malformed Mac OS partition table.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262178
9057	CVE-2011-1005	Medium		The safe-level feature in Ruby 1.8.6 through 1.8.6-420, 1.8.7 through 1.8.7-330, and 1.8.8dev allows context-dependent attackers to modify strings via the Exception#to_s method, as demonstrated by changing an intended pathname.	ruby.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262186
9058	CVE-2011-1004	Medium		The FileUtils.remove_entry_secure method in Ruby 1.8.6 through 1.8.6-420, 1.8.7 through 1.8.7-330, 1.8.8dev, 1.9.1 through 1.9.1-430, 1.9.2 through 1.9.2-136, and 1.9.3dev allows local users to delete arbitrary files via a symlink attack.	ruby.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262185
9059	CVE-2011-0999	Medium		mm/huge_memory.c in the Linux kernel before 2.6.38-rc5 does not prevent creation of a transparent huge page (THP) during the existence of a temporary stack for an exec system call, which allows local users to cause a denial of service (memory consumption) or possibly have unspecified other impact via a crafted application.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258698
9060	CVE-2011-0997	High		dhclient in ISC DHCP 3.0.x through 4.2.x before 4.2.1-P1, 3.1-ESV before 3.1-ESV-R1, and 4.1-ESV before 4.1-ESV-R2 allows remote attackers to execute arbitrary commands via shell metacharacters in a hostname obtained from a DHCP message.	dhcp.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266989
9061	CVE-2011-0987	Medium		The PMA_Bookmark_get function in libraries/bookmark.lib.php in phpMyAdmin 2.11.x before 2.11.11.3, and 3.3.x before 3.3.9.2, does not properly restrict bookmark queries, which makes it easier for remote authenticated users to trigger another user's execution of a SQL query by creating a bookmark.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325567
9062	CVE-2011-0986	Medium		phpMyAdmin 2.11.x before 2.11.11.2, and 3.3.x before 3.3.9.1, does not properly handle the absence of the (1) README, (2) ChangeLog, and (3) LICENSE files, which allows remote attackers to obtain the installation path via a direct request for a nonexistent file.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325566
9063	CVE-2011-0762	Medium		The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.	vsftpd.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262175
9064	CVE-2011-0761	Medium		Perl 5.10.x allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an ability to inject arguments into a (1) getpeername, (2) readdir, (3) closedir, (4) getsockname, (5) rewinddir, (6) tell, or (7) telldir function call.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	perl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277750
9065	CVE-2011-0755	Medium		Integer overflow in the mt_rand function in PHP before 5.3.4 might make it easier for context-dependent attackers to predict the return values by leveraging a script's use of a large max parameter, as demonstrated by a value that exceeds mt_getrandmax.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325959
9066	CVE-2011-0754	Medium		The SplFileInfo::getType function in the Standard PHP Library (SPL) extension in PHP before 5.3.4 on Windows does not properly detect symbolic links, which might make it easier for local users to conduct symlink attacks by leveraging cross-platform differences in the stat structure, related to lack of a FILE_ATTRIBUTE_REPARSE_POINT check.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325960
9067	CVE-2011-0753	Medium		Race condition in the PCNTL extension in PHP before 5.3.4, when a user-defined signal handler exists, might allow context-dependent attackers to cause a denial of service (memory corruption) via a large number of concurrent signals.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325961

	A	B	C	D	E	F	G	H	I	J	K	L	M
9068	CVE-2011-0726	Low		The do_task_stat function in fs/proc/array.c in the Linux kernel before 2.6.39-rc1 does not perform an expected uid check, which makes it easier for local users to defeat the ASLR protection mechanism by reading the start_code and end_code fields in the /proc/######/stat file for a process executing a PIE binary.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291631
9069	CVE-2011-0721	Medium		Multiple CRLF injection vulnerabilities in (1) chfn and (2) chsh in shadow 1:4.1.4 allow local users to add new users or groups to /etc/passwd via the GECOS field.	shadow.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258710
9070	CVE-2011-0719	Medium		Samba 3.x before 3.3.15, 3.4.x before 3.4.12, and 3.5.x before 3.5.7 does not perform range checks for file descriptors before use of the FD_SET macro, which allows remote attackers to cause a denial of service (stack memory corruption, and infinite loop or daemon crash) by opening a large number of files, related to (1) Winbind or (2) smbd.	The PATCH for it is GPLv3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262187
9071	CVE-2011-0716	Medium		The br_multicast_add_group function in net/bridge/br_multicast.c in the Linux kernel before 2.6.38, when a certain Ethernet bridge configuration is used, allows local users to cause a denial of service (memory corruption and system crash) by sending IGMP packets to a local interface.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359352
9072	CVE-2011-0714	Medium		Use-after-free vulnerability in a certain Red Hat patch for the RPC server sockets functionality in the Linux kernel 2.6.32 on Red Hat Enterprise Linux (RHEL) 6 might allow remote attackers to cause a denial of service (crash) via malformed data in a packet, related to lockd and the svc_xprt_received function.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277749
9073	CVE-2011-0712	Medium		Multiple buffer overflows in the caiaq Native Instruments USB audio functionality in the Linux kernel before 2.6.38-rc4-next-20110215 might allow attackers to cause a denial of service or possibly have unspecified other impact via a long USB device name, related to (1) the snd_usb_caiaq_audio_init function in sound/usb/caiaq/audio.c and (2) the snd_usb_caiaq_midi_init function in sound/usb/caiaq/midi.c.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258711
9074	CVE-2011-0711	Low		The xfs_fs_geometry function in fs/xfs/xfs_fsops.c in the Linux kernel before 2.6.38-rc6-git3 does not initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via an FSGEOMETRY_V1 ioctl call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262180
9075	CVE-2011-0710	Low		The task_show_regs function in arch/s390/kernel/traps.c in the Linux kernel before 2.6.38-rc4-next-20110216 on the s390 platform allows local users to obtain the values of the registers of an arbitrary process by reading a status file under /proc/.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258712
9076	CVE-2011-0709	Medium		The br_mdb_ip_get function in net/bridge/br_multicast.c in the Linux kernel before 2.6.35-rc5 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via an IGMP packet, related to lack of a multicast table.Per: http://cwe.mitre.org/data/definitions/476.html'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258700
9077	CVE-2011-0708	Medium		exif.c in the Exif extension in PHP before 5.3.6 on 64-bit platforms performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) via an image with a crafted Image File Directory (IFD) that triggers a buffer over-read.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325962
9078	CVE-2011-0695	Medium		Race condition in the cm_work_handler function in the InfiniBand driver (drivers/infiniband/core/cma.c) in Linux kernel 2.6.x allows remote attackers to cause a denial of service (panic) by sending an InfiniBand request while other request handlers are still running, which triggers an invalid pointer dereference.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262177
9079	CVE-2011-0640	High		The default configuration of udev on Linux does not warn the user before enabling additional Human Interface Device (HID) functionality over USB, which allows user-assisted attackers to execute arbitrary programs via crafted USB data, as demonstrated by keyboard and mouse data sent by malware on a smartphone that the user connected to the computer.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254772
9080	CVE-2011-0543	Low		Certain legacy functionality in fusermount in fuse 2.8.5 and earlier, when util-linux does not support the --no-canonicalize option, allows local users to bypass intended access restrictions and unmount arbitrary directories via a symlink attack.	fuse.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306457
9081	CVE-2011-0542	Low		fusermount in fuse 2.8.5 and earlier does not perform a chdir to / before performing a mount or umount, which allows local users to unmount arbitrary directories via unspecified vectors.	fuse.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306458
9082	CVE-2011-0541	Low		fuse 2.8.5 and earlier does not properly handle when /etc/mtab cannot be updated, which allows local users to unmount arbitrary directories via a symlink attack.	fuse.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306456
9083	CVE-2011-0539	Medium		The key_certify function in usr.bin/ssh/key.c in OpenSSH 5.6 and 5.7, when generating legacy certificates using the -t command-line option in ssh-keygen, does not initialize the nonce field, which might allow remote attackers to obtain sensitive stack memory contents or make it easier to conduct hash collision attacks.	openssh.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00255812

	A	B	C	D	E	F	G	H	I	J	K	L	M
9084	CVE-2011-0536	Medium		Multiple untrusted search path vulnerabilities in elf/dl-object.c in certain modified versions of the GNU C Library (aka glibc or libc6), including glibc-2.5-49.el5_5.6 and glibc-2.12-1.7.el6_0.3 in Red Hat Enterprise Linux, allow local users to gain privileges via a crafted dynamic shared object (DSO) in a subdirectory of the current working directory during execution of a (1) setuid or (2) setgid program that has $ORIGIN in (a) RPATH or (b) RUNPATH. NOTE: this issue exists because of an incorrect fix for CVE-2010-3847.Per: http://cwe.mitre.org/data/definitions/426.html 'CWE-426: Untrusted Search Path'	glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269489
9085	CVE-2011-0530	High		Buffer overflow in the mainloop function in nbd-server.c in the server in Network Block Device (nbd) before 2.9.20 might allow remote attackers to execute arbitrary code via a long request. NOTE: this issue exists because of a CVE-2005-3534 regression.	nbd.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258708
9086	CVE-2011-0521	Medium		The dvb_ca_ioctl function in drivers/media/dvb/ttpci/av7110_ca.c in the Linux kernel before 2.6.38-rc2 does not check the sign of a certain integer field, which allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact via a negative value.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254771
9087	CVE-2011-0465	High		xrdb.c in xrdb before 1.0.9 in X.Org X11R7.6 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in a hostname obtained from a (1) DHCP or (2) XDMCP message.	x11	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269525
9088	CVE-2011-0463	Low		The ocfs2_prepare_page_for_write function in fs/ocfs2/aops.c in the Oracle Cluster File System 2 (OCFS2) subsystem in the Linux kernel before 2.6.39-rc1 does not properly handle holes that cross page boundaries, which allows local users to obtain potentially sensitive information from uninitialized disk locations by reading a file.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269496
9089	CVE-2011-0433	Medium		Heap-based buffer overflow in the linetoken function in afmparse.c in t1lib, as used in teTeX 3.0.x, GNOME evince, and possibly other products, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a DVI file containing a crafted Adobe Font Metrics (AFM) file, a different vulnerability than CVE-2010-2642.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392013
9090	CVE-2011-0421	Medium		The _zip_name_locate function in zip_name_locate.c in the Zip extension in PHP before 5.3.6 does not properly handle a ZIPARCHIVE::FL_UNCHANGED argument, which might allow context-dependent attackers to cause a denial of service (NULL pointer dereference) via an empty ZIP archive that is processed with a (1) locateName or (2) statName operation.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325963
9091	CVE-2011-0414	High		ISC BIND 9.7.1 through 9.7.2-P3, when configured as an authoritative server, allows remote attackers to cause a denial of service (daemon hang) by sending a query at the time of (1) an IXFR transfer or (2) a DDNS update.	bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258695
9092	CVE-2011-0413	High		The DHCPv6 server in ISC DHCP 4.0.x and 4.1.x before 4.1.2-P1, 4.0-ESV and 4.1-ESV before 4.1-ESV-R1, and 4.2.x before 4.2.1b1 allows remote attackers to cause a denial of service (assertion failure and daemon crash) by sending a message over IPv6 for a declined and abandoned address.	isc dhcp.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254763
9093	CVE-2011-0408	Medium		pngrtran.c in libpng 1.5.x before 1.5.1 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted palette-based PNG image that triggers a buffer overflow, related to the png_do_expand_palette function, the png_do_rgb_to_gray function, and an integer underflow. NOTE: some of these details are obtained from third party information.	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254766
9094	CVE-2011-0343	Medium		Balabit syslog-ng 2.0, 3.0, 3.1, 3.2 OSE and PE, when running on FreeBSD or HP-UX, does not properly perform cast operations, which causes syslog-ng to use a default value of -1 to create log files with insecure permissions (07777), which allows local users to read and write to these log files.	syslog-ng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254782
9095	CVE-2011-0285	High		The process_chpw_request function in schpw.c in the password-changing functionality in kadmind in MIT Kerberos 5 (aka krb5) 1.7 through 1.9 frees an invalid pointer, which allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted request that triggers an error condition.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269488
9096	CVE-2011-0284	High		Double free vulnerability in the prepare_error_as function in do_as_req.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.7 through 1.9, when the PKINIT feature is enabled, allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via an e_data field containing typed data.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266363
9097	CVE-2011-0283	Medium		The Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.9 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a malformed request packet that does not trigger a response packet.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00255793
9098	CVE-2011-0282	Medium		The Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.6.x through 1.9, when an LDAP backend is used, allows remote attackers to cause a denial of service (NULL pointer dereference or buffer over-read, and daemon crash) via a crafted principal name.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00255794

	A	B	C	D	E	F	G	H	I	J	K	L	M
9099	CVE-2011-0281	Medium		The unparse implementation in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.6.x through 1.9, when an LDAP backend is used, allows remote attackers to cause a denial of service (file descriptor exhaustion and daemon hang) via a principal name that triggers use of a backslash escape sequence, as demonstrated by a \n sequence.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00255795
9100	CVE-2011-0226	High		Integer signedness error in psaux/t1decode.c in FreeType before 2.4.6, as used in CoreGraphics in Apple iOS before 4.2.9 and 4.3.x before 4.3.4 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted Type 1 font in a PDF document, as exploited in the wild in July 2011.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291616
9101	CVE-2011-0188	Medium		The VpMemAlloc function in bigdecimal.c in the BigDecimal class in Ruby 1.9.2-p136 and earlier, as used on Apple Mac OS X before 10.6.7 and other platforms, does not properly allocate memory, which allows context-dependent attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving creation of a large BigDecimal value within a 64-bit process, related to an integer truncation issue.	ruby.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266369
9102	CVE-2011-0064	Medium		The hb_buffer_ensure function in hb-buffer.c in HarfBuzz, as used in Pango 1.28.3, Firefox, and other products, does not verify that memory reallocations succeed, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly execute arbitrary code via crafted OpenType font data that triggers use of an incorrect index.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	pango.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262182
9103	CVE-2011-0020	High		Heap-based buffer overflow in the pango_ft2_font_render_box_glyph function in pango/pangoft2-render.c in libpango in Pango 1.28.3 and earlier, when the FreeType2 backend is enabled, allows user-assisted remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file, related to the glyph box for an FT_Bitmap object.	pango.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254776
9104	CVE-2011-0014	Medium		ssl/t1_lib.c in OpenSSL 0.9.8h through 0.9.8q and 1.0.0 through 1.0.0c allows remote attackers to cause a denial of service (crash), and possibly obtain sensitive information in applications that use OpenSSL, via a malformed ClientHello handshake message that triggers an out-of-bounds memory access, aka OCSP stapling vulnerability.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7596
9105	CVE-2011-0011	Medium		qemu-kvm before 0.11.0 disables VNC authentication when the password is cleared, which allows remote attackers to bypass authentication and establish VNC sessions.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359311
9106	CVE-2011-0010	Medium		check.c in sudo 1.7.x before 1.7.4p5, when a Runas group is configured, does not require a password for command execution that involves a gid change but no uid change, which allows local users to bypass an intended authentication requirement via the -g option to a sudo command.	sudo.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254781
9107	CVE-2011-0008	Medium		A certain Fedora patch for parse.c in sudo before 1.7.4p5-1.fc14 on Fedora 14 does not properly interpret a system group (aka %group) in the sudoers file during authorization decisions for a user who belongs to that group, which allows local users to leverage an applicable sudoers file and gain root privileges via a sudo command. NOTE: this vulnerability exists because of a CVE-2009-0034 regression.	sudo.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254780
9108	CVE-2011-0006	Low		The ima_lsm_rule_init function in security/integrity/ima/ima_policy.c in the Linux kernel before 2.6.37, when the Linux Security Modules (LSM) framework is disabled, allows local users to bypass Integrity Measurement Architecture (IMA) rules in opportunistic circumstances by leveraging an administrator's addition of an IMA rule for LSM.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359337
9109	CVE-2011-0002	Medium		libuser before 0.57 uses a cleartext password value of (1) !! or (2) x for new LDAP user accounts, which makes it easier for remote attackers to obtain access by specifying one of these values.	libuser.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254764
9110	CVE-2010-5332	High	CRITICAL	In the Linux kernel before 2.6.37, an out of bounds array access happened in drivers/net/mlx4/port.c. When searching for a free entry in either mlx4_register_vlan() or mlx4_register_mac(), and there is no free entry, the loop terminates without updating the local variable free thus causing out of array bounds access.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4550
9111	CVE-2010-5331	High	CRITICAL	In the Linux kernel before 2.6.34, a range check issue in drivers/gpu/drm/radeon/atombios.c could cause an off by one (buffer overflow) problem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4551
9112	CVE-2010-5329			The video_usercopy function in drivers/media/video/v4l2-ioctl.c in the Linux kernel before 2.6.39 relies on the count value of a v4l2_ext_controls data structure to determine a kmalloc size, which might allow local users to cause a denial of service (memory consumption) via a large value.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4072
9113	CVE-2010-5328	MEDIUM	Medium	include/linux/init_task.h in the Linux kernel before 2.6.35 does not prevent signals with a process group ID of zero from reaching the swapper process, which allows local users to cause a denial of service (system crash) by leveraging access to this process group.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3301
9114	CVE-2010-5325	High		Heap-based buffer overflow in the unhtmlify function in foomatic-rip in foomatic-filters before 4.0.6 allows remote attackers to cause a denial of service (memory corruption and crash) or possibly execute arbitrary code via a long job title.	foomatic-filters	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-462

	A	B	C	D	E	F	G	H	I	J	K	L	M
9115	CVE-2010-5321			Memory leak in drivers/media/video/videobuf-core.c in the videobuf subsystem in the Linux kernel 2.6.x through 4.x allows local users to cause a denial of service (memory consumption) by leveraging /dev/video access for a series of mmap calls that require new allocations, a different vulnerability than CVE-2007-6761. NOTE: as of 2016-06-18, this affects only 11 drivers that have not been updated to use videobuf2 instead of videobuf.	linux	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4095
9116	CVE-2010-5313	MEDIUM		Race condition in arch/x86/kvm/x86.c in the Linux kernel before 2.6.38 allows L2 guest OS users to cause a denial of service (L1 guest OS crash) via a crafted instruction that triggers an L2 emulation failure report, a similar issue to CVE-2014-7842.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-2142
9117	CVE-2010-5298	Medium		Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-7118
9118	CVE-2010-5107	Medium		The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login, which makes it easier for remote attackers to cause a denial of service (connection-slot exhaustion) by periodically making many new TCP connections.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00408771
9119	CVE-2010-5076	Medium		QSslSocket in Qt before 4.7.0-rc1 recognizes a wildcard IP address in the subject's Common Name field of an X.509 certificate, which might allow man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00362922
9120	CVE-2010-4833	Medium		Untrusted search path vulnerability in modules/engines/ms-windows/xp_theme.c in GTK+ before 2.24.0 allows local users to gain privileges via a Trojan horse uxtheme.dll file in the current working directory, a different vulnerability than CVE-2010-4831.Per: http://cwe.mitre.org/data/definitions/426.html 'CWE-426: Untrusted Search Path'	gtk+.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306459
9121	CVE-2010-4831	Medium		Untrusted search path vulnerability in gdk/win32/gdkinput-win32.c in GTK+ before 2.21.8 allows local users to gain privileges via a Trojan horse Wintab32.dll file in the current working directory.Per: http://cwe.mitre.org/data/definitions/426.html 'CWE-426: Untrusted Search Path'	gtk+.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00306460
9122	CVE-2010-4821	Medium		Cross-site scripting (XSS) vulnerability in phpMyFAQ before 2.6.9 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to index.php.	php	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00386297
9123	CVE-2010-4820	Low		Untrusted search path vulnerability in Ghostscript 8.62 allows local users to execute arbitrary PostScript code via a Trojan horse Postscript library file in Encoding/ under the current working directory, a different vulnerability than CVE-2010-2055.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-8678
9124	CVE-2010-4805	Medium		The socket implementation in net/core/sock.c in the Linux kernel before 2.6.35 does not properly manage a backlog of received packets, which allows remote attackers to cause a denial of service by sending a large amount of network traffic, related to the sk_add_backlog function and the sk_rmem_alloc socket field. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-4251.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281599
9125	CVE-2010-4777	Medium		The Perl_reg_numbered_buff_fetch function in Perl 5.10.0, 5.12.0, 5.14.0, and other versions, when running with debugging enabled, allows context-dependent attackers to cause a denial of service (assertion failure and application exit) via crafted input that is not properly handled when using certain regular expressions, as demonstrated by causing SpamAssassin and OCSInventory to crash.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6776
9126	CVE-2010-4755	Medium		The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262183
9127	CVE-2010-4708	High		The pam_env module in Linux-PAM (aka pam) 1.1.2 and earlier reads the .pam_environment file in a user's home directory, which might allow local users to run programs with an unintended environment by executing a program that relies on the pam_env PAM check.	linux-pam.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254775
9128	CVE-2010-4707	Medium		The check_acl function in pam_xauth.c in the pam_xauth module in Linux-PAM (aka pam) 1.1.2 and earlier does not verify that a certain ACL file is a regular file, which might allow local users to cause a denial of service (resource consumption) via a special file.	linux-pam.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254774
9129	CVE-2010-4706	Medium		The pam_sm_close_session function in pam_xauth.c in the pam_xauth module in Linux-PAM (aka pam) 1.1.2 and earlier does not properly handle a failure to determine a certain target uid, which might allow local users to delete unintended files by executing a program that relies on the pam_xauth PAM check.	linux-pam.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254774
9130	CVE-2010-4700	Medium		The set_magic_quotes_runtime function in PHP 5.3.2 and 5.3.3, when the MySQLi extension is used, does not properly interact with use of the mysqli_fetch_assoc function, which might make it easier for context-dependent attackers to conduct SQL injection attacks via crafted input that had been properly handled in earlier PHP versions.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325964

	A	B	C	D	E	F	G	H	I	J	K	L	M
9131	CVE-2010-4699	High		The iconv_mime_decode_headers function in the Iconv extension in PHP before 5.3.4 does not properly handle encodings that are unrecognized by the iconv and mbstring (aka Multibyte String) implementations, which allows remote attackers to trigger an incomplete output array, and possibly bypass spam detection or have unspecified other impact, via a crafted Subject header in an e-mail message, as demonstrated by the ks_c_5601-1987 character set.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325965
9132	CVE-2010-4698	Medium		Stack-based buffer overflow in the GD extension in PHP before 5.2.15 and 5.3.x before 5.3.4 allows context-dependent attackers to cause a denial of service (application crash) via vectors related to the imagepstext function and invalid anti-aliasing.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325966
9133	CVE-2010-4697	Medium		Use-after-free vulnerability in the Zend engine in PHP before 5.2.15 and 5.3.x before 5.3.4 might allow context-dependent attackers to cause a denial of service (heap memory corruption) or have unspecified other impact via vectors related to use of __set, __get, __isset, and __unset methods on objects accessed by a reference.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325967
9134	CVE-2010-4668	Medium		The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 2.6.37-rc7 allows local users to cause a denial of service (panic) via a zero-length I/O request in a device ioctl to a SCSI device, related to an unaligned map. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-4163.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252315
9135	CVE-2010-4665	Medium		Integer overflow in the ReadDirectory function in tiffdump.c in tiffdump in LibTIFF before 3.9.5 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TIFF file containing a directory data structure with many directory entries.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277729
9136	CVE-2010-4656	Medium		The iowarrior_write function in drivers/usb/misc/iowarrior.c in the Linux kernel before 2.6.37 does not properly allocate memory, which might allow local users to trigger a heap-based buffer overflow, and consequently cause a denial of service or gain privileges, via a long report.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291629
9137	CVE-2010-4655	Low		net/core/ethtool.c in the Linux kernel before 2.6.36 does not initialize certain data structures, which allows local users to obtain potentially sensitive information from kernel heap memory by leveraging the CAP_NET_ADMIN capability for an ethtool ioctl call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00291628
9138	CVE-2010-4651	Medium		Directory traversal vulnerability in util.c in GNU patch 2.6.1 and earlier allows user-assisted remote attackers to create or overwrite arbitrary files via a filename that is specified with a .. (dot dot) or full pathname, a related issue to CVE-2010-1679.	gnu gnu_patch.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00262176
9139	CVE-2010-4650	Medium		Buffer overflow in the fuse_do_ioctl function in fs/fuse/file.c in the Linux kernel before 2.6.37 allows local users to cause a denial of service or possibly have unspecified other impact by leveraging the ability to operate a CUSE server.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359344
9140	CVE-2010-4649	Medium		Integer overflow in the ib_uverbs_poll_cq function in drivers/infiniband/core/uverbs_cmd.c in the Linux kernel before 2.6.37 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact via a large value of a certain structure member.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00258699
9141	CVE-2010-4648	Low		The orinoco_ioctl_set_auth function in drivers/net/wireless/orinoco/wext.c in the Linux kernel before 2.6.37 does not properly implement a TKIP protection mechanism, which makes it easier for remote attackers to obtain access to a Wi-Fi network by reading Wi-Fi frames.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359346
9142	CVE-2010-4645	Medium		strtod.c, as used in the zend_strtod function in PHP 5.2 before 5.2.17 and 5.3 before 5.3.5, and other products, allows context-dependent attackers to cause a denial of service (infinite loop) via a certain floating-point value in scientific notation, which is not properly handled in x87 FPU registers.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325968
9143	CVE-2010-4565	Low		The bcm_connect function in net/can/bcm.c (aka the Broadcast Manager) in the Controller Area Network (CAN) implementation in the Linux kernel 2.6.36 and earlier creates a publicly accessible file with a filename containing a kernel memory address, which allows local users to obtain potentially sensitive information about kernel memory use by listing this filename.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249135
9144	CVE-2010-4563	Medium		The Linux kernel, when using IPv6, allows remote attackers to determine whether a host is sniffing the network by sending an ICMPv6 Echo Request to a multicast address and determining whether an Echo Reply is sent, as demonstrated by thcping.	linux kernel.	Unchanged	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	Won't Fix	WIND00334424
9145	CVE-2010-4531	Medium		Stack-based buffer overflow in the ATRDecodeAtr function in the Answer-to-Reset (ATR) Handler (atrhandler.c) for pcscd in PCSC-Lite 1.5.3, and possibly other 1.5.x and 1.6.x versions, allows physically proximate attackers to cause a denial of service (crash) and possibly execute arbitrary code via a smart card with an ATR message containing a long attribute value.	pcsc-lite.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254778
9146	CVE-2010-4530	Medium		Signedness error in ccid_serial.c in libccid in the USB Chip/Smart Card Interface Devices (CCID) driver, as used in pcscd in PCSC-Lite 1.5.3 and possibly other products, allows physically proximate attackers to execute arbitrary code via a smart card with a crafted serial number that causes a negative value to be used in a memcpy operation, which triggers a buffer overflow. NOTE: some sources refer to this issue as an integer overflow.	pcsc-lite.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254777
9147	CVE-2010-4529	Low		Integer underflow in the irda_getsockopt function in net/irda/af_irda.c in the Linux kernel before 2.6.37 on platforms other than x86 allows local users to obtain potentially sensitive information from kernel heap memory via an IRLMP_ENUMDEVICES getsockopt call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252310

	A	B	C	D	E	F	G	H	I	J	K	L	M
9148	CVE-2010-4527	Medium		The load_mixer_volumes function in sound/oss/soundcard.c in the OSS sound subsystem in the Linux kernel before 2.6.37 incorrectly expects that a certain name field ends with a '\0' character, which allows local users to conduct buffer overflow attacks and gain privileges, or possibly obtain sensitive information from kernel memory, via a SOUND_MIXER_SETLEVELS ioctl call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252309
9149	CVE-2010-4526	High		Race condition in the sctp_icmp_proto_unreachable function in net/sctp/input.c in Linux kernel 2.6.11-rc2 through 2.6.33 allows remote attackers to cause a denial of service (panic) via an ICMP unreachable message to a socket that is already locked by a user, which causes the socket to be freed and triggers list corruption, related to the sctp_wait_for_connect function.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249004
9150	CVE-2010-4525	Low		Linux kernel 2.6.33 and 2.6.34.y does not initialize the kvm_vcpu_events->interrupt.pad structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via unspecified vectors.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252314
9151	CVE-2010-4501	Medium		IO::Socket::SSL Perl module 1.35, when verify_mode is not VERIFY_NONE, fails open to VERIFY_NONE instead of throwing an error when a ca_file/ca_path cannot be verified, which allows remote attackers to bypass intended certificate restrictions.	io-socket-ssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247373
9152	CVE-2010-4494	High		Double free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00312304
9153	CVE-2010-4481	Medium		phpMyAdmin before 3.4.0-beta1 allows remote attackers to bypass authentication and obtain sensitive information via a direct request to phpinfo.php, which calls the phpinfo function.	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325564
9154	CVE-2010-4480	Medium		error.php in PhpMyAdmin 3.3.8.1 and earlier allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted BBcode tag containing @ characters, as demonstrated using [a@url@page].	phpMyAdmin	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325562
9155	CVE-2010-4478	High		OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.	openssh.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247360
9156	CVE-2010-4457	High		Unspecified vulnerability in Oracle Solaris 11 Express allows remote attackers to affect availability, related to SMB and CIFS.	WRLinux doesn't ship sun sunos.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235746
9157	CVE-2010-4409	Medium		Integer overflow in the NumberFormatter::getSymbol (aka numfmt_get_symbol) function in PHP 5.3.3 and earlier allows context-dependent attackers to cause a denial of service (application crash) via an invalid argument.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325969
9158	CVE-2010-4352	Low		Stack consumption vulnerability in D-Bus (aka DBus) before 1.4.1 allows local users to cause a denial of service (daemon crash) via a message containing many nested variants.	dbus.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249131
9159	CVE-2010-4347	Medium		The ACPI subsystem in the Linux kernel before 2.6.36.2 uses 0222 permissions for the debugfs custom_method file, which allows local users to gain privileges by placing a custom ACPI method in the ACPI interpreter tables, related to the acpi_debugfs_init function in drivers/acpi/debugfs.c.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249142
9160	CVE-2010-4346	Low		The install_special_mapping function in mm/mmap.c in the Linux kernel before 2.6.37-rc6 does not make an expected security_file_mmap function call, which allows local users to bypass intended mmap_min_addr restrictions and possibly conduct NULL pointer dereference attacks via a crafted assembly-language application.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249136
9161	CVE-2010-4343	Medium		drivers/scsi/bfa/bfa_core.c in the Linux kernel before 2.6.35 does not initialize a certain port data structure, which allows local users to cause a denial of service (system crash) via read operations on an fc_host statistics file.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249141
9162	CVE-2010-4342	High		The aun_incoming function in net/econet/af_econet.c in the Linux kernel before 2.6.37-rc6, when Econet is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and OOPS) by sending an Acorn Universal Networking (AUN) packet over UDP.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249134
9163	CVE-2010-4334	Medium		IO::Socket::SSL Perl module 1.35, when verify_mode is not VERIFY_NONE, fails open to VERIFY_NONE instead of throwing an error when a ca_file/ca_path cannot be verified, which allows remote attackers to bypass intended certificate restrictions.	io-socket-ssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252319
9164	CVE-2010-4263	High		The igb_receive_skb function in drivers/net/igb/igb_main.c in the Intel Gigabit Ethernet (aka igb) subsystem in the Linux kernel before 2.6.34, when Single Root I/O Virtualization (SR-IOV) and promiscuous mode are enabled but no VLANs are registered, allows remote attackers to cause a denial of service (NULL pointer dereference and panic) and possibly have unspecified other impact via a VLAN tagged frame.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254767
9165	CVE-2010-4258	Medium		The do_exit function in kernel/exit.c in the Linux kernel before 2.6.36.2 does not properly handle a KERNEL_DS get_fs value, which allows local users to bypass intended access_ok restrictions, overwrite arbitrary kernel memory locations, and gain privileges by leveraging a (1) BUG, (2) NULL pointer dereference, or (3) page fault, as demonstrated by vectors involving the clear_child_tid feature and the splice system call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249140

	A	B	C	D	E	F	G	H	I	J	K	L	M
9166	CVE-2010-4256	Low		The pipe_fcntl function in fs/pipe.c in the Linux kernel before 2.6.37 does not properly determine whether a file is a named pipe, which allows local users to cause a denial of service via an F_SETPIPE_SZ fcntl call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254768
9167	CVE-2010-4252	High		OpenSSL before 1.0.0c, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247359
9168	CVE-2010-4251	Medium		The socket implementation in net/core/sock.c in the Linux kernel before 2.6.34 does not properly manage a backlog of received packets, which allows remote attackers to cause a denial of service (memory consumption) by sending a large amount of network traffic, as demonstrated by netperf UDP tests.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00281600
9169	CVE-2010-4250	Medium		Memory leak in the inotify_init1 function in fs/inotify/inotify_user.c in the Linux kernel before 2.6.37 allows local users to cause a denial of service (memory consumption) via vectors involving failed attempts to create files.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00359312
9170	CVE-2010-4249	Medium		The wait_for_unix_gc function in net/unix/garbage.c in the Linux kernel before 2.6.37-rc3-next-20101125 does not properly select times for garbage collection of inflight sockets, which allows local users to cause a denial of service (system hang) via crafted use of the socketpair and sendmsg system calls for SOCK_SEQPACKET sockets.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00245439
9171	CVE-2010-4248	Medium		Race condition in the __exit_signal function in kernel/exit.c in the Linux kernel before 2.6.37-rc2 allows local users to cause a denial of service via vectors related to multithreaded exec, the use of a thread group leader in kernel/posix-cpu-timers.c, and the selection of a new thread group leader in the de_thread function in fs/exec.c.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00245438
9172	CVE-2010-4243	Medium		fs/exec.c in the Linux kernel before 2.6.37 does not enable the OOM Killer to assess use of stack memory by arrays representing the (1) arguments and (2) environment, which allows local users to cause a denial of service (memory consumption) via a crafted exec system call, aka an OOM dodging issue, a related issue to CVE-2010-3858.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254765
9173	CVE-2010-4242	Medium		The hci_uart_tty_open function in the HCI UART driver (drivers/bluetooth/hci_ldisc.c) in the Linux kernel 2.6.36, and possibly other versions, does not verify whether the tty has a write operation, which allows local users to cause a denial of service (NULL pointer dereference) via vectors related to the Bluetooth driver.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252311
9174	CVE-2010-4237	MEDIUM	MEDIUM	Mercurial before 1.6.4 fails to verify the Common Name field of SSL certificates which allows remote attackers who acquire a certificate signed by a Certificate Authority to perform a man-in-the-middle attack.	mercurial	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5180
9175	CVE-2010-4226	Medium		cpio, as used in build 2007.05.10, 2010.07.28, and possibly other versions, allows remote attackers to overwrite arbitrary files via a symlink within an RPM package archive.	cpio	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6783
9176	CVE-2010-4180	Medium		OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the downgrade to an unintended cipher via vectors involving sniffing network traffic to discover a session identifier.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247372
9177	CVE-2010-4176	Medium		plymouth-pretrigger.sh in dracut and udev, when running on Fedora 13 and 14, sets insecure permissions for the /dev/systty device file, which allows remote authenticated users to read terminal data from tty0 for local users.	udev.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247371
9178	CVE-2010-4175	Medium		Integer overflow in the rds_cmsg_rdma_args function (net/rds/rdma.c) in Linux kernel 2.6.35 allows local users to cause a denial of service (crash) and possibly trigger memory corruption via a crafted Reliable Datagram Sockets (RDS) request, a different vulnerability than CVE-2010-3865.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252312
9179	CVE-2010-4169	Medium		Use-after-free vulnerability in mm/mprotect.c in the Linux kernel before 2.6.37-rc2 allows local users to cause a denial of service via vectors involving an mprotect system call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00245442
9180	CVE-2010-4167	Medium		Untrusted search path vulnerability in configure.c in ImageMagick before 6.6.5-5, when MAGICKCORE_INSTALLED_SUPPORT is defined, allows local users to gain privileges via a Trojan horse configuration file in the current working directory.Per: http://cwe.mitre.org/data/definitions/426.html 'CWE-426: Untrusted Search Path'	imagemagick.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00245437
9181	CVE-2010-4165	Medium		The do_tcp_setsockopt function in net/ipv4/tcp.c in the Linux kernel before 2.6.37-rc2 does not properly restrict TCP_MAXSEG (aka MSS) values, which allows local users to cause a denial of service (OOPS) via a setsockopt call that specifies a small value, leading to a divide-by-zero error or incorrect use of a signed integer.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00245443
9182	CVE-2010-4164	High		Multiple integer underflows in the x25_parse_facilities function in net/x25/x25_facilities.c in the Linux kernel before 2.6.36.2 allow remote attackers to cause a denial of service (system crash) via malformed X.25 (1) X25_FAC_CLASS_A, (2) X25_FAC_CLASS_B, (3) X25_FAC_CLASS_C, or (4) X25_FAC_CLASS_D facility data, a different vulnerability than CVE-2010-3873.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252316
9183	CVE-2010-4163	Medium		The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 2.6.36.2 allows local users to cause a denial of service (panic) via a zero-length I/O request in a device ioctl to a SCSI device.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252317

	A	B	C	D	E	F	G	H	I	J	K	L	M
9184	CVE-2010-4162	Medium		Multiple integer overflows in fs/bio.c in the Linux kernel before 2.6.36.2 allow local users to cause a denial of service (system crash) via a crafted device ioctl to a SCSI device.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00297832
9185	CVE-2010-4161	Medium		The udp_queue_rcv_skb function in net/ipv4/udp.c in a certain Red Hat build of the Linux kernel 2.6.18 in Red Hat Enterprise Linux (RHEL) 5 allows attackers to cause a denial of service (deadlock and system hang) by sending UDP traffic to a socket that has a crafted socket filter, a related issue to CVE-2010-4158.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249143
9186	CVE-2010-4160	Medium		Multiple integer overflows in the (1) pppol2tp_sendmsg function in net/l2tp/l2tp_ppp.c, and the (2) l2tp_ip_sendmsg function in net/l2tp/l2tp_ip.c, in the PPPoL2TP and IPoL2TP implementations in the Linux kernel before 2.6.36.2 allow local users to cause a denial of service (heap memory corruption and panic) or possibly gain privileges via a crafted sendto call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00241279
9187	CVE-2010-4158	Low		The sk_run_filter function in net/core/filter.c in the Linux kernel before 2.6.36.2 does not check whether a certain memory location has been initialized before executing a (1) BPF_S_LD_MEM or (2) BPF_S_LDX_MEM instruction, which allows local users to obtain potentially sensitive information from kernel stack memory via a crafted socket filter.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249133
9188	CVE-2010-4157	Medium		Integer overflow in the ioc_general function in drivers/scsi/gdth.c in the Linux kernel before 2.6.36.1 on 64-bit platforms allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact via a large argument in an ioctl call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00241280
9189	CVE-2010-4150	Medium		Double free vulnerability in the imap_do_open function in the IMAP extension (ext/imap/php_imap.c) in PHP 5.2 before 5.2.15 and 5.3 before 5.3.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325971
9190	CVE-2010-4083	Low		The copy_semid_to_user function in ipc/sem.c in the Linux kernel before 2.6.36 does not initialize a certain structure, which allows local users to obtain potentially sensitive information from kernel stack memory via a (1) IPC_INFO, (2) SEM_INFO, (3) IPC_STAT, or (4) SEM_STAT command in a semctl system call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238383
9191	CVE-2010-4082	Low		The viafb_ioctl_get_viafb_info function in drivers/video/via/ioctl.c in the Linux kernel before 2.6.36-rc5 does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via a VIAFB_GET_INFO ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238375
9192	CVE-2010-4081	Low		The snd_hdspm_hwdep_ioctl function in sound/pci/rme9652/hdspm.c in the Linux kernel before 2.6.36-rc6 does not initialize a certain structure, which allows local users to obtain potentially sensitive information from kernel stack memory via an SNDRV_HDSPM_IOCTL_GET_CONFIG_INFO ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238374
9193	CVE-2010-4080	Low		The snd_hdsp_hwdep_ioctl function in sound/pci/rme9652/hdsp.c in the Linux kernel before 2.6.36-rc6 does not initialize a certain structure, which allows local users to obtain potentially sensitive information from kernel stack memory via an SNDRV_HDSP_IOCTL_GET_CONFIG_INFO ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238373
9194	CVE-2010-4079	Low		The ivtvfb_ioctl function in drivers/media/video/ivtv/ivtvfb.c in the Linux kernel before 2.6.36-rc8 does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via an FBIOGET_VBLANK ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238372
9195	CVE-2010-4078	Low		The sisfb_ioctl function in drivers/video/sis/sis_main.c in the Linux kernel before 2.6.36-rc6 does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via an FBIOGET_VBLANK ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238368
9196	CVE-2010-4077	Low		The ntty_ioctl_tiocgicount function in drivers/char/nozomi.c in the Linux kernel 2.6.36.1 and earlier does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via a TIOCGICOUNT ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238369
9197	CVE-2010-4076	Low		The rs_ioctl function in drivers/char/amiserial.c in the Linux kernel 2.6.36.1 and earlier does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via a TIOCGICOUNT ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238358
9198	CVE-2010-4075	Low		The uart_get_count function in drivers/serial/serial_core.c in the Linux kernel before 2.6.37-rc1 does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via a TIOCGICOUNT ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238362
9199	CVE-2010-4074	Low		The USB subsystem in the Linux kernel before 2.6.36-rc5 does not properly initialize certain structure members, which allows local users to obtain potentially sensitive information from kernel stack memory via vectors related to TIOCGICOUNT ioctl calls, and the (1) mos7720_ioctl function in drivers/usb/serial/mos7720.c and (2) mos7840_ioctl function in drivers/usb/serial/mos7840.c.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238363

	A	B	C	D	E	F	G	H	I	J	K	L	M
9200	CVE-2010-4073	Low		The ipc subsystem in the Linux kernel before 2.6.37-rc1 does not initialize certain structures, which allows local users to obtain potentially sensitive information from kernel stack memory via vectors related to the (1) compat_sys_semctl, (2) compat_sys_msgctl, and (3) compat_sys_shmctl functions in ipc/compat.c; and the (4) compat_sys_mq_open and (5) compat_sys_mq_getsetattr functions in ipc/compat_mq.c.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238361
9201	CVE-2010-4072	Low		The copy_shmid_to_user function in ipc/shm.c in the Linux kernel before 2.6.37-rc1 does not initialize a certain structure, which allows local users to obtain potentially sensitive information from kernel stack memory via vectors related to the shmctl system call and the old shm interface.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238357
9202	CVE-2010-4054	Medium		The gs_type2_interpret function in Ghostscript allows remote attackers to cause a denial of service (incorrect pointer dereference and application crash) via crafted font data in a compressed data stream, aka bug 691043.	The PATCH for it is GPLv3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00240006
9203	CVE-2010-4052	Medium		Stack consumption vulnerability in the regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (resource exhaustion) via a regular expression containing adjacent repetition operators, as demonstrated by a {10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD.	gnu glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252307
9204	CVE-2010-4051	Medium		The regcomp implementation in the GNU C Library (aka glibc or libc6) through 2.11.3, and 2.12.x through 2.12.2, allows context-dependent attackers to cause a denial of service (application crash) via a regular expression containing adjacent bounded repetitions that bypass the intended RE_DUP_MAX limitation, as demonstrated by a {10,}{10,}{10,}{10,}{10,} sequence in the proftpd.gnu.c exploit for ProFTPD, related to a RE_DUP_MAX overflow.	gnu glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00252308
9205	CVE-2010-4022	Medium		The do_standalone function in the MIT krb5 KDC database propagation daemon (kpropd) in Kerberos 1.7, 1.8, and 1.9, when running in standalone mode, does not properly handle when a worker child process exits abnormally, which allows remote attackers to cause a denial of service (listening process termination, no new connections, and lack of updates in slave KVC) via unspecified vectors.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00255792
9206	CVE-2010-4021	Low		The Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.7 does not properly restrict the use of TGT credentials for armoring TGS requests, which might allow remote authenticated users to impersonate a client by rewriting an inner request, aka a KrbFastReq forgery issue.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247363
9207	CVE-2010-4020	Low		MIT Kerberos 5 (aka krb5) 1.8.x through 1.8.3 does not reject RC4 key-derivation checksums, which might allow remote authenticated users to forge a (1) AD-SIGNEDPATH or (2) AD-KDC-ISSUED signature, and possibly gain privileges, by leveraging the small key space that results from certain one-byte stream-cipher operations.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247361
9208	CVE-2010-4015	Medium		Buffer overflow in the gettoken function in contrib/intarray/_int_bool.c in the intarray array module in PostgreSQL 9.0.x before 9.0.3, 8.4.x before 8.4.7, 8.3.x before 8.3.14, and 8.2.x before 8.2.20 allows remote authenticated users to cause a denial of service (crash) and possibly execute arbitrary code via integers with a large number of digits to unspecified functions.	postgresql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00254779
9209	CVE-2010-4008	Medium		libxml2 before 2.7.8, as used in Google Chrome before 7.0.517.44, Apple Safari 5.0.2 and earlier, and other products, reads from invalid memory locations during processing of malformed XPath expressions, which allows context-dependent attackers to cause a denial of service (application crash) via a crafted XML document.	libxml2.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237797
9210	CVE-2010-3914	High		Untrusted search path vulnerability in VIM Development Group GVim before 7.3.034, and possibly other versions before 7.3.46, allows local users, and possibly remote attackers, to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse User32.dll or other DLL that is located in the same folder as a .TXT file. NOTE: some of these details are obtained from third party information.Per: http://cwe.mitre.org/data/definitions/426.html 'CWE-426: Untrusted Search Path'	vim	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00242276
9211	CVE-2010-3904	High		The rds_page_copy_user function in net/rds/page.c in the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel before 2.6.36 does not properly validate addresses obtained from user space, which allows local users to gain privileges via crafted use of the sendmsg and recvmsg system calls.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237798
9212	CVE-2010-3881	Low		arch/x86/kvm/x86.c in the Linux kernel before 2.6.36.2 does not initialize certain structure members, which allows local users to obtain potentially sensitive information from kernel stack memory via read operations on the /dev/kvm device.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00240433
9213	CVE-2010-3880	Medium		net/ipv4/inet_diag.c in the Linux kernel before 2.6.37-rc2 does not properly audit INET_DIAG bytecode, which allows local users to cause a denial of service (kernel infinite loop) via crafted INET_DIAG_REQ_BYTECODE instructions in a netlink message that contains multiple attribute elements, as demonstrated by INET_DIAG_BC_JMP instructions.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00240429
9214	CVE-2010-3879	Medium		FUSE, possibly 2.8.5 and earlier, allows local users to create mtab entries with arbitrary pathnames, and consequently unmount any filesystem, via a symlink attack on the parent directory of the mountpoint of a FUSE filesystem, a different vulnerability than CVE-2010-0789.	fuse.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00240430

	A	B	C	D	E	F	G	H	I	J	K	L	M
9215	CVE-2010-3877	Low		The get_name function in net/tipc/socket.c in the Linux kernel before 2.6.37-rc2 does not initialize a certain structure, which allows local users to obtain potentially sensitive information from kernel stack memory by reading a copy of this structure.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00239967
9216	CVE-2010-3876	Low		net/packet/af_packet.c in the Linux kernel before 2.6.37-rc2 does not properly initialize certain structure members, which allows local users to obtain potentially sensitive information from kernel stack memory by leveraging the CAP_NET_RAW capability to read copies of the applicable structures.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00239966
9217	CVE-2010-3875	Low		The ax25_getname function in net/ax25/af_ax25.c in the Linux kernel before 2.6.37-rc2 does not initialize a certain structure, which allows local users to obtain potentially sensitive information from kernel stack memory by reading a copy of this structure.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00239965
9218	CVE-2010-3874	Medium		Heap-based buffer overflow in the bcm_connect function in net/can/bcm.c (aka the Broadcast Manager) in the Controller Area Network (CAN) implementation in the Linux kernel before 2.6.36.2 on 64-bit platforms might allow local users to cause a denial of service (memory corruption) via a connect operation.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00239964
9219	CVE-2010-3873	High		The X.25 implementation in the Linux kernel before 2.6.36.2 does not properly parse facilities, which allows remote attackers to cause a denial of service (heap memory corruption and panic) or possibly have unspecified other impact via malformed (1) X25_FAC_CALLING_AE or (2) X25_FAC_CALLED_AE data, related to net/x25/x25_facilities.c and net/x25/x25_in.c, a different vulnerability than CVE-2010-4164.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00239963
9220	CVE-2010-3872	High		The apr_status_t fcgid_header_bucket_read function in fcgid_bucket.c in Apache mod_fcgid before 2.3.6 does not use bytewise pointer arithmetic in certain circumstances, which has unknown impact and attack vectors related to untrusted FastCGI applications and a stack buffer overwrite.	Apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00245436
9221	CVE-2010-3870	Medium		The utf8_decode function in PHP before 5.3.4 does not properly handle non-shortest form UTF-8 encoding and ill-formed subsequences in UTF-8 data, which makes it easier for remote attackers to bypass cross-site scripting (XSS) and SQL injection protection mechanisms via a crafted string.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325972
9222	CVE-2010-3865	High		Integer overflow in the rds_rdma_pages function in net/rds/rdma.c in the Linux kernel allows local users to cause a denial of service (crash) and possibly execute arbitrary code via a crafted iovec struct in a Reliable Datagram Sockets (RDS) request, which triggers a buffer overflow.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00239303
9223	CVE-2010-3864	High		Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00240428
9224	CVE-2010-3861	Low		The ethtool_get_rxnfc function in net/core/ethtool.c in the Linux kernel before 2.6.36 does not initialize a certain block of heap memory, which allows local users to obtain potentially sensitive information via an ETHTOOL_GRXCLSRLALL ethtool command with a large info.rule_cnt value, a different vulnerability than CVE-2010-2478.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238356
9225	CVE-2010-3859	Medium		Multiple integer signedness errors in the TIPC implementation in the Linux kernel before 2.6.36.2 allow local users to gain privileges via a crafted sendmsg call that triggers a heap-based buffer overflow, related to the tipc_msg_build function in net/tipc/msg.c and the verify_iovec function in net/core/iovec.c.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237799
9226	CVE-2010-3858	Medium		The setup_arg_pages function in fs/exec.c in the Linux kernel before 2.6.36, when CONFIG_STACK_GROWSDOWN is used, does not properly restrict the stack memory consumption of the (1) arguments and (2) environment for a 32-bit application on a 64-bit platform, which allows local users to cause a denial of service (system crash) via a crafted exec system call, a related issue to CVE-2010-2240.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237800
9227	CVE-2010-3856	High		ld.so in the GNU C Library (aka glibc or libc6) before 2.11.3, and 2.12.x before 2.12.2, does not properly restrict use of the LD_AUDIT environment variable to reference dynamic shared objects (DSOs) as audit objects, which allows local users to gain privileges by leveraging an unsafe DSO located in a trusted library directory, as demonstrated by libpcprofile.so.	gnu glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236966
9228	CVE-2010-3855	Medium		Buffer overflow in the ft_var_readpackedpoints function in truetype/ttgxvar.c in FreeType 2.4.3 and earlier allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted TrueType GX font.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237563
9229	CVE-2010-3853	Medium		pam_namespace.c in the pam_namespace module in Linux-PAM (aka pam) before 1.1.3 uses the environment of the invoking application or service during execution of the namespace.init script, which might allow local users to gain privileges by running a setuid program that relies on the pam_namespace PAM check, as demonstrated by the sudo program.	linux-pam.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237564
9230	CVE-2010-3850	High		The ec_dev_ioctl function in net/econet/af_econet.c in the Linux kernel before 2.6.36.2 does not require the CAP_NET_ADMIN capability, which allows local users to bypass intended access restrictions and configure econet addresses via an SIOCSIFADDR ioctl call.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236961

	A	B	C	D	E	F	G	H	I	J	K	L	M
9231	CVE-2010-3849	Medium		The econet_sendmsg function in net/econet/af_econet.c in the Linux kernel before 2.6.36.2, when an econet address is configured, allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a sendmsg call that specifies a NULL value for the remote address field.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236959
9232	CVE-2010-3848	Medium		Stack-based buffer overflow in the econet_sendmsg function in net/econet/af_econet.c in the Linux kernel before 2.6.36.2, when an econet address is configured, allows local users to gain privileges by providing a large number of iovec structures.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236958
9233	CVE-2010-3847	Medium		elf/dl-load.c in ld.so in the GNU C Library (aka glibc or libc6) through 2.11.2, and 2.12.x through 2.12.1, does not properly handle a value of $ORIGIN for the LD_AUDIT environment variable, which allows local users to gain privileges via a crafted dynamic shared object (DSO) located in an arbitrary directory.	gnu glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236966
9234	CVE-2010-3842	Medium		Absolute path traversal vulnerability in curl 7.20.0 through 7.21.1, when the --remote-header-name or -J option is used, allows remote servers to create or overwrite arbitrary files by using \ (backslash) as a separator of path components within the Content-disposition HTTP header.	Curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236437
9235	CVE-2010-3840	Medium		The Gis_line_string::init_from_wkb function in sql/spatial.cc in MySQL 5.1 before 5.1.51 allows remote authenticated users to cause a denial of service (server crash) by calling the PolyFromWKB function with Well-Known Binary (WKB) data containing a crafted number of (1) line strings or (2) line points.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235676
9236	CVE-2010-3839	Medium		MySQL 5.1 before 5.1.51 and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (infinite loop) via multiple invocations of a (1) prepared statement or (2) stored procedure that creates a query with nested JOIN statements.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235675
9237	CVE-2010-3838	Medium		MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via a query that uses the (1) GREATEST or (2) LEAST function with a mixed list of numeric and LONGBLOB arguments, which is not properly handled when the function's result is processed using an intermediate temporary table.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235674
9238	CVE-2010-3837	Medium		MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via a prepared statement that uses GROUP_CONCAT with the WITH ROLLUP modifier, probably triggering a use-after-free error when a copied object is modified in a way that also affects the original object.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235673
9239	CVE-2010-3836	Medium		MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (assertion failure and server crash) via vectors related to view preparation, pre-evaluation of LIKE predicates, and IN Optimizers.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235670
9240	CVE-2010-3835	Medium		MySQL 5.1 before 5.1.51 and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (mysqld server crash) by performing a user-variable assignment in a logical expression that is calculated and stored in a temporary table for GROUP BY, then causing the expression value to be used after the table is created, which causes the expression to be re-evaluated instead of accessing its value from the table.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235669
9241	CVE-2010-3834	Medium		Unspecified vulnerability in MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 allows remote authenticated users to cause a denial of service (server crash) via vectors related to materializing a derived table that required a temporary table for grouping and user variable assignments.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235668
9242	CVE-2010-3833	Medium		MySQL 5.0 before 5.0.92, 5.1 before 5.1.51, and 5.5 before 5.5.6 does not properly propagate type errors, which allows remote attackers to cause a denial of service (server crash) via crafted arguments to extreme-value functions such as (1) LEAST and (2) GREATEST, related to KILL_BAD_DATA and a CREATE TABLE ... SELECT.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235667
9243	CVE-2010-3814	Medium		Heap-based buffer overflow in the Ins_SHZ function in ttinterp.c in FreeType 2.4.3 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted SHZ bytecode instruction, related to TrueType opcodes, as demonstrated by a PDF document with a crafted embedded font.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237559
9244	CVE-2010-3781	Medium		The PL/php add-on 1.4 and earlier for PostgreSQL does not properly protect script execution by a different SQL user identity within the same session, which allows remote authenticated users to gain privileges via crafted script code in a SECURITY DEFINER function, a related issue to CVE-2010-3433.	PostgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236083
9245	CVE-2010-3762	Medium		ISC BIND before 9.7.2-P2, when DNSSEC validation is enabled, does not properly handle certain bad signatures if multiple trust anchors exist for a single zone, which allows remote attackers to cause a denial of service (daemon crash) via a DNS query.	Isc bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237155
9246	CVE-2010-3710	Medium		Stack consumption vulnerability in the filter_var function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3, when FILTER_VALIDATE_EMAIL mode is used, allows remote attackers to cause a denial of service (memory consumption and application crash) via a long e-mail address string.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325974

	A	B	C	D	E	F	G	H	I	J	K	L	M
9247	CVE-2010-3709	Medium		The ZipArchive::getArchiveComment function in PHP 5.2.x through 5.2.14 and 5.3.x through 5.3.3 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ZIP archive.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325975
9248	CVE-2010-3705	High		The sctp_auth_asoc_get_hmac function in net/sctp/auth.c in the Linux kernel before 2.6.36 does not properly validate the hmac_ids array of an SCTP peer, which allows remote attackers to cause a denial of service (memory corruption and panic) via a crafted value in the last element of this array.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235662
9249	CVE-2010-3698	Medium		The KVM implementation in the Linux kernel before 2.6.36 does not properly reload the FS and GS segment registers, which allows host OS users to cause a denial of service (host OS crash) via a KVM_RUN ioctl call in conjunction with a modified Local Descriptor Table (LDT).	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00245441
9250	CVE-2010-3697	Medium		The wait_for_child_to_die function in main/event.c in FreeRADIUS 2.1.x before 2.1.10, in certain circumstances involving long-term database outages, does not properly handle long queue times for requests, which allows remote attackers to cause a denial of service (daemon crash) by sending many requests.	Freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235661
9251	CVE-2010-3696	Medium		The fr_dhcp_decode function in lib/dhcp.c in FreeRADIUS 2.1.9, in certain non-default builds, does not properly handle the DHCP Relay Agent Information option, which allows remote attackers to cause a denial of service (infinite loop and daemon outage) via a packet that has more than one sub-option. NOTE: some of these details are obtained from third party information.	Freeradius	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235660
9252	CVE-2010-3683	Medium		Oracle MySQL 5.1 before 5.1.49 and 5.5 before 5.5.5 sends an OK packet when a LOAD DATA INFILE request generates SQL errors, which allows remote authenticated users to cause a denial of service (mysqld daemon crash) via a crafted request.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234858
9253	CVE-2010-3682	Medium		Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) by using EXPLAIN with crafted SELECT ... UNION ... ORDER BY (SELECT ... WHERE ...) statements, which triggers a NULL pointer dereference in the Item_singlerow_subselect::store function.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234856
9254	CVE-2010-3681	Medium		Oracle MySQL 5.1 before 5.1.49 and 5.5 before 5.5.5 allows remote authenticated users to cause a denial of service (mysqld daemon crash) by using the HANDLER interface and performing alternate reads from two indexes on a table, which triggers an assertion failure.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234855
9255	CVE-2010-3680	Medium		Oracle MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (mysqld daemon crash) by creating temporary tables with nullable columns while using InnoDB, which triggers an assertion failure.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234852
9256	CVE-2010-3679	Medium		Oracle MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (mysqld daemon crash) via certain arguments to the BINLOG command, which triggers an access of uninitialized memory, as demonstrated by valgrind.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234853
9257	CVE-2010-3678	Medium		Oracle MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (crash) via (1) IN or (2) CASE operations with NULL arguments that are explicitly specified or indirectly provided by the WITH ROLLUP modifier.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234850
9258	CVE-2010-3677	Medium		Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) via a join query that uses a table with a unique SET column.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234851
9259	CVE-2010-3676	Medium		storage/innobase/dict/dict0crea.c in mysqld in Oracle MySQL 5.1 before 5.1.49 allows remote authenticated users to cause a denial of service (assertion failure) by modifying the (1) innodb_file_format or (2) innodb_file_per_table configuration parameters for the InnoDB storage engine, then executing a DDL statement.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234849
9260	CVE-2010-3616	Medium		ISC DHCP server 4.2 before 4.2.0-P2, when configured to use failover partnerships, allows remote attackers to cause a denial of service (communications-interrupted state and DHCP client service loss) by connecting to a port that is only intended for a failover peer, as demonstrated by a Nagios check_tcp process check to TCP port 520.	isc dhcp.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00249132
9261	CVE-2010-3615	Medium		named in ISC BIND 9.7.2-P2 does not check all intended locations for allow-query ACLs, which might allow remote attackers to make successful requests for private DNS records via the standard DNS query mechanism.	bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247370
9262	CVE-2010-3614	Medium		named in ISC BIND 9.x before 9.6.2-P3, 9.7.x before 9.7.2-P3, 9.4-ESV before 9.4-ESV-R4, and 9.6-ESV before 9.6-ESV-R3 does not properly determine the security status of an NS RRset during a DNSKEY algorithm rollover, which might allow remote attackers to cause a denial of service (DNSSEC validation error) by triggering a rollover.	bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247369
9263	CVE-2010-3613	Medium		named in ISC BIND 9.6.2 before 9.6.2-P3, 9.6-ESV before 9.6-ESV-R3, and 9.7.x before 9.7.2-P3 does not properly handle the combination of signed negative responses and corresponding RRSIG records in the cache, which allows remote attackers to cause a denial of service (daemon crash) via a query for cached data.	bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247368

	A	B	C	D	E	F	G	H	I	J	K	L	M
9264	CVE-2010-3611	Medium		ISC DHCP server 4.0 before 4.0.2, 4.1 before 4.1.2, and 4.2 before 4.2.0-P1 allows remote attackers to cause a denial of service (crash) via a DHCPv6 packet containing a Relay-Forward message without an address in the Relay-Forward link-address field.	isc dhcp.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00242274
9265	CVE-2010-3495	Medium		Race condition in ZEO/StorageServer.py in Zope Object Database (ZODB) before 3.10.0 allows remote attackers to cause a denial of service (daemon outage) by establishing and then immediately closing a TCP connection, leading to the accept function having an unexpected return value of None, an unexpected value of None for the address, or an ECONNABORTED, EAGAIN, or EWOULDBLOCK error, a related issue to CVE-2010-3492.	python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234380
9266	CVE-2010-3494	Medium		Race condition in the FTPHandler class in ftpserver.py in pyftpdlib before 0.5.2 allows remote attackers to cause a denial of service (daemon outage) by establishing and then immediately closing a TCP connection, leading to the accept function having an unexpected value of None for the address, or an ECONNABORTED, EAGAIN, or EWOULDBLOCK error, a related issue to CVE-2010-3492.	WRLinux doesn't ship g.rodola pyftpdlib.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234379
9267	CVE-2010-3493	Medium		Multiple race conditions in smtpd.py in the smtpd module in Python 2.6, 2.7, 3.1, and 3.2 alpha allow remote attackers to cause a denial of service (daemon outage) by establishing and then immediately closing a TCP connection, leading to the accept function having an unexpected return value of None, an unexpected value of None for the address, or an ECONNABORTED, EAGAIN, or EWOULDBLOCK error, or the getpeername function having an ENOTCONN error, a related issue to CVE-2010-3492.	python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234377
9268	CVE-2010-3492	Medium		The asyncore module in Python before 3.2 does not properly handle unsuccessful calls to the accept function, and does not have accompanying documentation describing how daemon applications should handle unsuccessful calls to the accept function, which makes it easier for remote attackers to conduct denial of service attacks that terminate these applications via network connections.	python.	Unchanged	8.0.0.14	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234376
9269	CVE-2010-3477	Low		The tcf_act_police_dump function in net/sched/act_police.c in the actions implementation in the network queueing functionality in the Linux kernel before 2.6.36-rc4 does not properly initialize certain structure members, which allows local users to obtain potentially sensitive information from kernel memory via vectors involving a dump operation. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2942.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235878
9270	CVE-2010-3448	Medium		drivers/platform/x86/thinkpad_acpi.c in the Linux kernel before 2.6.34 on ThinkPad devices, when the X.Org X server is used, does not properly restrict access to the video output control state, which allows local users to cause a denial of service (system hang) via a (1) read or (2) write operation.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235666
9271	CVE-2010-3442	Medium		Multiple integer overflows in the snd_ctl_new function in sound/core/control.c in the Linux kernel before 2.6.36-rc5-next-20100929 allow local users to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted (1) SNDRV_CTL_IOCTL_ELEM_ADD or (2) SNDRV_CTL_IOCTL_ELEM_REPLACE ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235659
9272	CVE-2010-3437	Medium		Integer signedness error in the pkt_find_dev_from_minor function in drivers/block/pktcdvd.c in the Linux kernel before 2.6.36-rc6 allows local users to obtain sensitive information from kernel memory or cause a denial of service (invalid pointer dereference and system crash) via a crafted index value in a PKT_CTRL_CMD_STATUS ioctl call.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234848
9273	CVE-2010-3436	Medium		fopen_wrappers.c in PHP 5.3.x through 5.3.3 might allow remote attackers to bypass open_basedir restrictions via vectors related to the length of a filename.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325976
9274	CVE-2010-3435	Medium		The (1) pam_env and (2) pam_mail modules in Linux-PAM (aka pam) before 1.1.2 use root privileges during read access to files and directories that belong to arbitrary user accounts, which might allow local users to obtain sensitive information by leveraging this filesystem activity, as demonstrated by a symlink attack on the .pam_environment file in a user's home directory.	linux-pam.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234644
9275	CVE-2010-3433	Medium		The PL/perl and PL/Tcl implementations in PostgreSQL 7.4 before 7.4.30, 8.0 before 8.0.26, 8.1 before 8.1.22, 8.2 before 8.2.18, 8.3 before 8.3.12, 8.4 before 8.4.5, and 9.0 before 9.0.1 do not properly protect script execution by a different SQL user identity within the same session, which allows remote authenticated users to gain privileges via crafted script code in a SECURITY DEFINER function, as demonstrated by (1) redefining standard functions or (2) redefining operators, a different vulnerability than CVE-2010-1168, CVE-2010-1169, CVE-2010-1170, and CVE-2010-1447.	Postgresql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236083
9276	CVE-2010-3432	High		The sctp_packet_config function in net/sctp/output.c in the Linux kernel before 2.6.35.6 performs extraneous initializations of packet data structures, which allows remote attackers to cause a denial of service (panic) via a certain sequence of SCTP traffic.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234381

	A	B	C	D	E	F	G	H	I	J	K	L	M
9277	CVE-2010-3431	Medium		The privilege-dropping implementation in the (1) pam_env and (2) pam_mail modules in Linux-PAM (aka pam) 1.1.2 does not check the return value of the setfsuid system call, which might allow local users to obtain sensitive information by leveraging an unintended uid, as demonstrated by a symlink attack on the .pam_environment file in a user's home directory. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-3435.	linux-pam.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234373
9278	CVE-2010-3430	Medium		The privilege-dropping implementation in the (1) pam_env and (2) pam_mail modules in Linux-PAM (aka pam) 1.1.2 does not perform the required setfsgid and setgroups system calls, which might allow local users to obtain sensitive information by leveraging unintended group permissions, as demonstrated by a symlink attack on the .pam_environment file in a user's home directory. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-3435.	linux-pam.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234372
9279	CVE-2010-3389	Medium		The (1) SAPDatabase and (2) SAPInstance scripts in OCF Resource Agents (aka resource-agents or cluster-agents) 1.0.3 in Linux-HA place a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse shared library in the current working directory.	resource_agents.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00240007
9280	CVE-2010-3373			paxtest handles temporary files insecurely	paxtest	Unchanged	Investigate	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-11703
9281	CVE-2010-3316	Low		The run_coprocess function in pam_xauth.c in the pam_xauth module in Linux-PAM (aka pam) before 1.1.2 does not check the return values of the setuid, setgid, and setgroups system calls, which might allow local users to read arbitrary files by executing a program that relies on the pam_xauth PAM check.	linux-pam.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234371
9282	CVE-2010-3315	Medium		authz.c in the mod_dav_svn module for the Apache HTTP Server, as distributed in Apache Subversion 1.5.x before 1.5.8 and 1.6.x before 1.6.13, when SVNPathAuthz short_circuit is enabled, does not properly handle a named repository as a rule scope, which allows remote authenticated users to bypass intended access restrictions via svn commands.	Apache.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237160
9283	CVE-2010-3311	High		Integer overflow in base/ftstream.c in libXft (aka the X FreeType library) in FreeType before 2.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted Compact Font Format (CFF) font file that triggers a heap-based buffer overflow, related to an input stream position error issue, a different vulnerability than CVE-2010-1797.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234502
9284	CVE-2010-3310	Low		Multiple integer signedness errors in net/rose/af_rose.c in the Linux kernel before 2.6.36-rc5-next-20100923 allow local users to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a rose_getname function call, related to the rose_bind and rose_connect functions.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00233945
9285	CVE-2010-3301	High		The IA32 system call emulation functionality in arch/x86/ia32/ia32entry.S in the Linux kernel before 2.6.36-rc4-git2 on the x86_64 platform does not zero extend the %eax register after the 32-bit entry path to ptrace is used, which allows local users to gain privileges by triggering an out-of-bounds access to the system call table using the %rax register. NOTE: this vulnerability exists because of a CVE-2007-4573 regression.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00233531
9286	CVE-2010-3298	Medium		The hso_get_count function in drivers/net/usb/hso.c in the Linux kernel before 2.6.36-rc5 does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via a TIOCGICOUNT ioctl call.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00233532
9287	CVE-2010-3297	Medium		The eql_g_master_cfg function in drivers/net/eql.c in the Linux kernel before 2.6.36-rc5 does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via an EQL_GETMASTRCFG ioctl call.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00233530
9288	CVE-2010-3296	Medium		The cxgb_extension_ioctl function in drivers/net/cxgb3/cxgb3_main.c in the Linux kernel before 2.6.36-rc5 does not properly initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via a CHELSIO_GET_QSET_NUM ioctl call.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00233529
9289	CVE-2010-3192	Low		Certain run-time memory protection mechanisms in the GNU C Library (aka glibc or libc6) print argv[0] and backtrace information, which might allow context-dependent attackers to obtain sensitive information from process memory by executing an incorrect program, as demonstrated by a setuid program that contains a stack-based buffer overflow error, related to the __fortify_fail function in debug/fortify_fail.c, and the __stack_chk_fail (aka stack protection) and __chk_fail (aka FORTIFY_SOURCE) implementations.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231599
9290	CVE-2010-3170	Medium		Mozilla Firefox before 3.5.14 and 3.6.x before 3.6.11, Thunderbird before 3.0.9 and 3.1.x before 3.1.5, and SeaMonkey before 2.0.9 recognize a wildcard IP address in the subject's Common Name field of an X.509 certificate, which might allow man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234638
9291	CVE-2010-3087	Medium		LibTIFF before 3.9.2-5.2.1 in SUSE openSUSE 11.3 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted TIFF image.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232834

	A	B	C	D	E	F	G	H	I	J	K	L	M
9292	CVE-2010-3086	Medium		include/asm-x86/futex.h in the Linux kernel before 2.6.25 does not properly implement exception fixup, which allows local users to cause a denial of service (panic) via an invalid application that triggers a page fault.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00241272
9293	CVE-2010-3084	High		Buffer overflow in the niu_get_ethtool_tcam_all function in drivers/net/niu.c in the Linux kernel before 2.6.36-rc4 allows local users to cause a denial of service or possibly have unspecified other impact via the ETHTOOL_GRXCLSRLALL ethtool command.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232669
9294	CVE-2010-3081	High		The compat_alloc_user_space functions in include/asm/compat.h files in the Linux kernel before 2.6.36-rc4-git2 on 64-bit platforms do not properly allocate the userspace memory required for the 32-bit compatibility layer, which allows local users to gain privileges by leveraging the ability of the compat_mc_getsockopt function (aka the MCAST_MSFILTER getsockopt support) to control a certain length value, related to a stack pointer underflow issue, as exploited in the wild in September 2010.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00233536
9295	CVE-2010-3080	Medium		Double free vulnerability in the snd_seq_oss_open function in sound/core/seq/oss/seq_oss_init.c in the Linux kernel before 2.6.36-rc4 might allow local users to cause a denial of service or possibly have unspecified other impact via an unsuccessful attempt to open the /dev/sequencer device.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232170
9296	CVE-2010-3079	Medium		kernel/trace/ftrace.c in the Linux kernel before 2.6.35.5, when debugfs is enabled, does not properly handle interaction between mutex possession and llseek operations, which allows local users to cause a denial of service (outage of all function tracing files) via an lseek call on a file descriptor associated with the set_ftrace_filter file.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232101
9297	CVE-2010-3078	Low		The xfs_ioc_fsgetxattr function in fs/xfs/linux-2.6/xfs_ioctl.c in the Linux kernel before 2.6.36-rc4 does not initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via an ioctl call.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232100
9298	CVE-2010-3069	High		Stack-based buffer overflow in the (1) sid_parse and (2) dom_sid_parse functions in Samba before 3.5.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted Windows Security ID (SID) on a file share.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232497
9299	CVE-2010-3067	Medium		Integer overflow in the do_io_submit function in fs/aio.c in the Linux kernel before 2.6.36-rc4-next-20100915 allows local users to cause a denial of service or possibly have unspecified other impact via crafted use of the io_submit system call.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00235879
9300	CVE-2010-3066	Medium		The io_submit_one function in fs/aio.c in the Linux kernel before 2.6.23 allows local users to cause a denial of service (NULL pointer dereference) via a crafted io_submit system call with an IOCB_FLAG_RESFD flag.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247367
9301	CVE-2010-3065	Medium		The default session serializer in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 does not properly handle the PS_UNDEF_MARKER marker, which allows context-dependent attackers to modify arbitrary session variables via a crafted session variable name.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325977
9302	CVE-2010-3064	Medium		Stack-based buffer overflow in the php_mysqlnd_auth_write function in the Mysqlnd extension in PHP 5.3 through 5.3.2 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long (1) username or (2) database name argument to the (a) mysql_connect or (b) mysqli_connect function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325980
9303	CVE-2010-3063	Medium		The php_mysqlnd_read_error_from_line function in the Mysqlnd extension in PHP 5.3 through 5.3.2 does not properly calculate a buffer length, which allows context-dependent attackers to trigger a heap-based buffer overflow via crafted inputs that cause a negative length value to be used.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325980
9304	CVE-2010-3062	Medium		mysqlnd_wireprotocol.c in the Mysqlnd extension in PHP 5.3 through 5.3.2 allows remote attackers to (1) read sensitive memory via a modified length value, which is not properly handled by the php_mysqlnd_ok_read function; or (2) trigger a heap-based buffer overflow via a modified length value, which is not properly handled by the php_mysqlnd_rset_header_read function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325981
9305	CVE-2010-3054	Medium		Unspecified vulnerability in FreeType 2.3.9, and other versions before 2.4.2, allows remote attackers to cause a denial of service via vectors involving nested Standard Encoding Accented Character (aka seac) calls, related to psaux.h, cffgload.c, cffgload.h, and t1decode.c.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232301
9306	CVE-2010-3053	Medium		bdf/bdflib.c in FreeType before 2.4.2 allows remote attackers to cause a denial of service (application crash) via a crafted BDF font file, related to an attempted modification of a value in a static string.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00230116
9307	CVE-2010-3015	Medium		Integer overflow in the ext4_ext_get_blocks function in fs/ext4/extents.c in the Linux kernel before 2.6.34 allows local users to cause a denial of service (BUG and system crash) via a write operation on the last block of a large file, followed by a sync operation.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00228348
9308	CVE-2010-2965	High		The WDB target agent debug service in Wind River VxWorks 6.x, 5.x, and earlier, as used on the Rockwell Automation 1756-ENBT series A with firmware 3.2.6 and 3.6.1 and other products, allows remote attackers to read or modify arbitrary memory locations, perform function calls, or manage tasks via requests to UDP port 17185, a related issue to CVE-2005-3804.	The WDB target agent debug service	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00228512

	A	B	C	D	E	F	G	H	I	J	K	L	M
9309	CVE-2010-2963	Medium		drivers/media/video/v4l2-compat-ioctl32.c in the Video4Linux (V4L) implementation in the Linux kernel before 2.6.36 on 64-bit platforms does not validate the destination of a memory copy operation, which allows local users to write to arbitrary kernel memory locations, and consequently gain privileges, via a VIDIOCSTUNER ioctl call on a /dev/video device, followed by a VIDIOCSMICROCODE ioctl call on this device.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236955
9310	CVE-2010-2962	High		drivers/gpu/drm/i915/i915_gem.c in the Graphics Execution Manager (GEM) in the Intel i915 driver in the Direct Rendering Manager (DRM) subsystem in the Linux kernel before 2.6.36 does not properly validate pointers to blocks of memory, which allows local users to write to arbitrary kernel memory locations, and consequently gain privileges, via crafted use of the ioctl interface, related to (1) pwrite and (2) pread operations.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00245440
9311	CVE-2010-2960	High		The keyctl_session_to_parent function in security/keys/keyctl.c in the Linux kernel 2.6.35.4 and earlier expects that a certain parent session keyring exists, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a KEYCTL_SESSION_TO_PARENT argument to the keyctl function.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231601
9312	CVE-2010-2959	High		Integer overflow in net/can/bcm.c in the Controller Area Network (CAN) implementation in the Linux kernel before 2.6.27.53, 2.6.32.x before 2.6.32.21, 2.6.34.x before 2.6.34.6, and 2.6.35.x before 2.6.35.4 allows attackers to execute arbitrary code or cause a denial of service (system crash) via crafted CAN traffic.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00229594
9313	CVE-2010-2956	Medium		Sudo 1.7.0 through 1.7.4p3, when a Runas group is configured, does not properly handle use of the -u option in conjunction with the -g option, which allows local users to gain privileges via a command line containing a -u root sequence.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232098
9314	CVE-2010-2955	Low		The cfg80211_wext_giwessid function in net/wireless/wext-compat.c in the Linux kernel before 2.6.36-rc3-next-20100831 does not properly initialize certain structure members, which allows local users to leverage an off-by-one error in the ioctl_standard_iw_point function in net/wireless/wext-core.c, and obtain potentially sensitive information from kernel heap memory, via vectors involving an SIOCGIWESSID ioctl call that specifies a large buffer size.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231595
9315	CVE-2010-2954	Medium		The irda_bind function in net/irda/af_irda.c in the Linux kernel before 2.6.36-rc3-next-20100901 does not properly handle failure of the irda_open_tsap function, which allows local users to cause a denial of service (NULL pointer dereference and panic) and possibly have unspecified other impact via multiple unsuccessful calls to bind on an AF_IRDA (aka PF_IRDA) socket.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231598
9316	CVE-2010-2950	Medium		Format string vulnerability in stream.c in the phar extension in PHP 5.3.x through 5.3.3 allows context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted phar:// URI that is not properly handled by the phar_stream_flush function, leading to errors in the php_stream_wrapper_log_error function. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-2094.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325997
9317	CVE-2010-2949	Medium		bgpd in Quagga before 0.99.17 does not properly parse AS paths, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unknown AS type in an AS path attribute in a BGP UPDATE message.	Quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00230574
9318	CVE-2010-2948	Medium		Stack-based buffer overflow in the bgp_route_refresh_receive function in bgp_packet.c in bgpd in Quagga before 0.99.17 allows remote authenticated users to cause a denial of service (daemon crash) or possibly execute arbitrary code via a malformed Outbound Route Filtering (ORF) record in a BGP ROUTE-REFRESH (RR) message.	Quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00230573
9319	CVE-2010-2946	Low		fs/jfs/xattr.c in the Linux kernel before 2.6.35.2 does not properly handle a certain legacy format for storage of extended attributes, which might allow local users by bypass intended xattr namespace restrictions via an os2. substring at the beginning of a name.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00229595
9320	CVE-2010-2943	High		The xfs implementation in the Linux kernel before 2.6.35 does not look up inode allocation btrees before reading inode buffers, which allows remote authenticated users to read unlinked files, or read or overwrite disk blocks that are currently assigned to an active file but were previously assigned to an unlinked file, by accessing a stale NFS filehandle.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00229329
9321	CVE-2010-2942	Low		The actions implementation in the network queueing functionality in the Linux kernel before 2.6.36-rc2 does not properly initialize certain structure members when performing dump operations, which allows local users to obtain potentially sensitive information from kernel memory via vectors related to (1) the tcf_gact_dump function in net/sched/act_gact.c, (2) the tcf_mirred_dump function in net/sched/act_mirred.c, (3) the tcf_nat_dump function in net/sched/act_nat.c, (4) the tcf_simp_dump function in net/sched/act_simple.c, and (5) the tcf_skbedit_dump function in net/sched/act_skbedit.c.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00229328
9322	CVE-2010-2941	High		ipp.c in cupsd in CUPS 1.4.4 and earlier does not properly allocate memory for attribute values with invalid string data types, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly execute arbitrary code via a crafted IPP request.	Cups.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00238354

	A	B	C	D	E	F	G	H	I	J	K	L	M
9323	CVE-2010-2939	Medium		Double free vulnerability in the ssl3_get_key_exchange function in the OpenSSL client (ssl/s3_clnt.c) in OpenSSL 1.0.0a, 0.9.8, 0.9.7, and possibly other versions, when using ECDH, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted private key with an invalid prime. NOTE: some sources refer to this as a use-after-free issue.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00228114
9324	CVE-2010-2938	Medium		arch/x86/hvm/vmx/vmcs.c in the virtual-machine control structure (VMCS) implementation in the Linux kernel 2.6.18 on Red Hat Enterprise Linux (RHEL) 5, when an Intel platform without Extended Page Tables (EPT) functionality is used, accesses VMCS fields without verifying hardware support for these fields, which allows local users to cause a denial of service (host OS crash) by requesting a VMCS dump for a fully virtualized Xen guest.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237157
9325	CVE-2010-2808	Medium		Buffer overflow in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.4.2 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted Adobe Type 1 Mac Font File (aka LWFN) font.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00227245
9326	CVE-2010-2807	Medium		FreeType before 2.4.2 uses incorrect integer data types during bounds checking, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00227244
9327	CVE-2010-2806	Medium		Array index error in the t42_parse_sfnts function in type42/t42parse.c in FreeType before 2.4.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via negative size values for certain strings in FontType42 font files, leading to a heap-based buffer overflow.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00227242
9328	CVE-2010-2805	Medium		The FT_Stream_EnterFrame function in base/ftstream.c in FreeType before 2.4.2 does not properly validate certain position values, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00227241
9329	CVE-2010-2803	Low		The drm_ioctl function in drivers/gpu/drm/drm_drv.c in the Direct Rendering Manager (DRM) subsystem in the Linux kernel before 2.6.27.53, 2.6.32.x before 2.6.32.21, 2.6.34.x before 2.6.34.6, and 2.6.35.x before 2.6.35.4 allows local users to obtain potentially sensitive information from kernel memory by requesting a large memory-allocation amount.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00233663
9330	CVE-2010-2799	Medium		Stack-based buffer overflow in the nestlex function in nestlex.c in Socat 1.5.0.0 through 1.7.1.2 and 2.0.0-b1 through 2.0.0-b3, when bidirectional data relay is enabled, allows context-dependent attackers to execute arbitrary code via long command-line arguments.	socat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00226253
9331	CVE-2010-2798	High		The gfs2_dirent_find_space function in fs/gfs2/dir.c in the Linux kernel before 2.6.35 uses an incorrect size value in calculations associated with sentinel directory entries, which allows local users to cause a denial of service (NULL pointer dereference and panic) and possibly have unspecified other impact by renaming a file in a GFS2 filesystem, related to the gfs2_rename function in fs/gfs2/ops_inode.c.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00226252
9332	CVE-2010-2791	Medium		mod_proxy in httpd in Apache HTTP Server 2.2.9, when running on Unix, does not close the backend connection if a timeout occurs when reading a response from a persistent connection, which allows remote attackers to obtain a potentially sensitive response intended for a different client in opportunistic circumstances via a normal HTTP request. NOTE: this is the same issue as CVE-2010-2068, but for a different OS and set of affected versions.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00226052
9333	CVE-2010-2784	Medium		The subpage MMIO initialization functionality in the subpage_register function in exec.c in QEMU-KVM, as used in the Hypervisor (aka rhev-hypervisor) in Red Hat Enterprise Virtualization (RHEV) 2.2 and KVM 83, does not properly select the index for access to the callback array, which allows guest OS users to cause a denial of service (guest OS crash) or possibly gain privileges via unspecified vectors.	kvm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232308
9334	CVE-2010-2783			IcedTea6 before 1.7.4 allow unsigned apps to read and write arbitrary files, related to Extended JNLP Services.	icedtea6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-11582
9335	CVE-2010-2653	Medium		Race condition in the hvc_close function in drivers/char/hvc_console.c in the Linux kernel before 2.6.34 allows local users to cause a denial of service or possibly have unspecified other impact by closing a Hypervisor Virtual Console device, related to the hvc_open and hvc_remove functions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202825
9336	CVE-2010-2631	Medium		LibTIFF 3.9.0 ignores tags in certain situations during the first stage of TIFF file processing and does not properly handle this during the second stage, which allows remote attackers to cause a denial of service (application crash) via a crafted file, a different vulnerability than CVE-2010-2481.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221132
9337	CVE-2010-2630	Medium		The TIFFReadDirectory function in LibTIFF 3.9.0 does not properly validate the data types of codec-specific tags that have an out-of-order position in a TIFF file, which allows remote attackers to cause a denial of service (application crash) via a crafted file, a different vulnerability than CVE-2010-2481.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221132
9338	CVE-2010-2621	Medium		The QSslSocketBackendPrivate::transmit function in src_network_ssl_qsslsocket_openssl.cpp in Qt 4.6.3 and earlier allows remote attackers to cause a denial of service (infinite loop) via a malformed request.	qt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223986

	A	B	C	D	E	F	G	H	I	J	K	L	M
9339	CVE-2010-2598	Medium		LibTIFF in Red Hat Enterprise Linux (RHEL) 3 on x86_64 platforms, as used in tiff2rgba, attempts to process image data even when the required compression functionality is not configured, which allows remote attackers to cause a denial of service via a crafted TIFF image, related to downsampled OJPEG input.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221324
9340	CVE-2010-2597	Medium		The TIFFVStripSize function in tif_strip.c in LibTIFF 3.9.0 and 3.9.2 makes incorrect calls to the TIFFGetField function, which allows remote attackers to cause a denial of service (application crash) via a crafted TIFF image, related to downsampled OJPEG input and possibly related to a compiler optimization that triggers a divide-by-zero error.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221321
9341	CVE-2010-2596	Medium		The OJPEGPostDecode function in tif_ojpeg.c in LibTIFF 3.9.0 and 3.9.2, as used in tiff2ps, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted TIFF image, related to downsampled OJPEG input.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221322
9342	CVE-2010-2595	Medium		The TIFFYCbCrtoRGB function in LibTIFF 3.9.0 and 3.9.2, as used in ImageMagick, does not properly handle invalid ReferenceBlackWhite values, which allows remote attackers to cause a denial of service (application crash) via a crafted TIFF image that triggers an array index error, related to downsampled OJPEG input.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221319
9343	CVE-2010-2548			IcedTea6 before 1.7.4 does not properly check property access, which allows unsigned apps to read and write arbitrary files.	icedtea6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN7-11581
9344	CVE-2010-2547	Medium		Use-after-free vulnerability in kbx/keybox-blob.c in GPGSM in GnuPG 2.x through 2.0.16 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a certificate with a large number of Subject Alternate Names, which is not properly handled in a realloc operation when importing the certificate or verifying its signature.	gnupg.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00225296
9345	CVE-2010-2542	High		Stack-based buffer overflow in the is_git_directory function in setup.c in Git before 1.7.2.1 allows local users to gain privileges via a long gitdir: field in a .git file in a working copy.	git.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00224919
9346	CVE-2010-2541	Medium		Buffer overflow in ftmulti.c in the ftmulti demo program in FreeType before 2.4.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00224920
9347	CVE-2010-2538	Medium		Integer overflow in the btrfs_ioctl_clone function in fs/btrfs/ioctl.c in the Linux kernel before 2.6.35 might allow local users to obtain sensitive information via a BTRFS_IOC_CLONE_RANGE ioctl call.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00224654
9348	CVE-2010-2537	Medium		The btrfs_ioctl_clone function in fs/btrfs/ioctl.c in the Linux kernel before 2.6.35 allows local users to overwrite an append-only file via a (1) BTRFS_IOC_CLONE or (2) BTRFS_IOC_CLONE_RANGE ioctl call that specifies this file as a donor.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00224653
9349	CVE-2010-2533	REJECT		** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2010-2621. Reason: This candidate is a reservation duplicate of CVE-2010-2621. Notes: All CVE users should reference CVE-2010-2621 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.		Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223987
9350	CVE-2010-2531	Medium		The var_export function in PHP 5.2 before 5.2.14 and 5.3 before 5.3.3 flushes the output buffer to the user when certain fatal errors occur, even if display_errors is off, which allows remote attackers to obtain sensitive information by causing the application to exceed limits for memory, execution time, or recursion.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325986
9351	CVE-2010-2529	Medium		Unspecified vulnerability in ping.c in iputils 20020927, 20070202, 20071127, and 20100214 on Mandriva Linux allows remote attackers to cause a denial of service (hang) via a crafted echo response.	iputils.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223791
9352	CVE-2010-2527	Medium		Multiple buffer overflows in demo programs in FreeType before 2.4.0 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223583
9353	CVE-2010-2526	Medium		The cluster logical volume manager daemon (clvmd) in lvm2-cluster in LVM2 before 2.02.72, as used in Red Hat Global File System (GFS) and other products, does not verify client credentials upon a socket connection, which allows local users to cause a denial of service (daemon exit or logical-volume change) or possibly have unspecified other impact via crafted control commands.	lvm2.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00228513
9354	CVE-2010-2524	Medium		The DNS resolution functionality in the CIFS implementation in the Linux kernel before 2.6.35, when CONFIG_CIFS_DFS_UPCALL is enabled, relies on a user's keyring for the dns_resolver upcall in the cifs.upcall userspace helper, which allows local users to spoof the results of DNS queries and perform arbitrary CIFS mounts via vectors involving an add_key call, related to a cache stuffing issue and MS-DFS referrals.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00226086
9355	CVE-2010-2523	High		Multiple buffer overflows in ha.c in the mipv6 daemon in UMIP 0.4 allow remote attackers to have an unspecified impact via a crafted (1) ND_OPT_PREFIX_INFORMATION or (2) ND_OPT_HOME_AGENT_INFO packet.	linux-ipv6 umip.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223152
9356	CVE-2010-2522	Low		The mipv6 daemon in UMIP 0.4 does not verify that netlink messages originated in the kernel, which allows local users to spoof netlink socket communication via a crafted unicast message.	linux-ipv6 umip.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223151

	A	B	C	D	E	F	G	H	I	J	K	L	M
9357	CVE-2010-2521	High		Multiple buffer overflows in fs/nfsd/nfs4xdr.c in the XDR implementation in the NFS server in the Linux kernel before 2.6.34-rc6 allow remote attackers to cause a denial of service (panic) or possibly execute arbitrary code via a crafted NFSv4 compound WRITE request, related to the read_buf and nfsd4_decode_compound functions.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223155
9358	CVE-2010-2520	Medium		Heap-based buffer overflow in the Ins_IUP function in truetype/ttinterp.c in FreeType before 2.4.0, when TrueType bytecode support is enabled, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223164
9359	CVE-2010-2519	Medium		Heap-based buffer overflow in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.4.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted length value in a POST fragment header in a font file.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223163
9360	CVE-2010-2500	Medium		Integer overflow in the gray_render_span function in smooth/ftgrays.c in FreeType before 2.4.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223162
9361	CVE-2010-2499	Medium		Buffer overflow in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.4.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted LaserWriter PS font file with an embedded PFB fragment.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223161
9362	CVE-2010-2498	Medium		The psh_glyph_find_strong_points function in pshinter/pshalgo.c in FreeType before 2.4.0 does not properly implement hinting masks, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted font file that triggers an invalid free operation.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223160
9363	CVE-2010-2497	Medium		Integer underflow in glyph handling in FreeType before 2.4.0 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font file.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223158
9364	CVE-2010-2495	High		The pppol2tp_xmit function in drivers/net/pppol2tp.c in the L2TP implementation in the Linux kernel before 2.6.34 does not properly validate certain values associated with an interface, which allows attackers to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via vectors related to a routing change.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00220093
9365	CVE-2010-2492	Medium		Buffer overflow in the ecryptfs_uid_hash macro in fs/ecryptfs/messaging.c in the eCryptfs subsystem in the Linux kernel before 2.6.35 might allow local users to gain privileges or cause a denial of service (system crash) via unspecified vectors.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221674
9366	CVE-2010-2489	High		Buffer overflow in Ruby 1.9.x before 1.9.1-p429 on Windows might allow local users to gain privileges via a crafted ARGF.inplace_mode value that is not properly handled when constructing the filenames of the backup files.	ruby-lang ruby.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221672
9367	CVE-2010-2483	Medium		The TIFFRGBAImageGet function in LibTIFF 3.9.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a TIFF file with an invalid combination of SamplesPerPixel and Photometric values.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221134
9368	CVE-2010-2482	Medium		LibTIFF 3.9.4 and earlier does not properly handle an invalid td_stripbytecount field, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted TIFF file, a different vulnerability than CVE-2010-2443.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221133
9369	CVE-2010-2481	Medium		The TIFFExtractData macro in LibTIFF before 3.9.4 does not properly handle unknown tag types in TIFF directory entries, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted TIFF file.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221132
9370	CVE-2010-2478	High		Integer overflow in the ethtool_get_rxnfc function in net/core/ethtool.c in the Linux kernel before 2.6.33.7 on 32-bit platforms allows local users to cause a denial of service or possibly have unspecified other impact via an ETHTOOL_GRXCLSRLALL ethtool command with a large info.rule_cnt value that triggers a buffer overflow, a different vulnerability than CVE-2010-3084.	Linux Kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00220607
9371	CVE-2010-2477	Medium		Multiple cross-site scripting (XSS) vulnerabilities in the paste.httpexceptions implementation in Paste before 1.7.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving a 404 status code, related to (1) paste.urlparser.StaticURLParser, (2) paste.urlparser.PkgResourcesParser, (3) paste.urlmap.URLMap, and (4) HTTPNotFound.	pythonpaste paste.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00242275
9372	CVE-2010-2443	Medium		Unspecified vulnerability in LibTIFF before 3.9.3 allows remote attackers to cause a denial of service (application crash) via an OJPEG image with undefined strip offsets.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221104
9373	CVE-2010-2432	Medium		The cupsDoAuthentication function in auth.c in the client in CUPS before 1.4.4, when HAVE_GSSAPI is omitted, does not properly handle a demand for authorization, which allows remote CUPS servers to cause a denial of service (infinite loop) via HTTP_UNAUTHORIZED responses.	cups.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00222228
9374	CVE-2010-2431	Medium		The cupsFileOpen function in CUPS before 1.4.4 allows local users, with lp group membership, to overwrite arbitrary files via a symlink attack on the (1) /var/cache/cups/remote.cache or (2) /var/cache/cups/job.cache file.	cups.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00222230

	A	B	C	D	E	F	G	H	I	J	K	L	M
9375	CVE-2010-2387	Low		vicious-extensions/ve-misc.c in GNOME Display Manager (gdm) 2.20.x before 2.20.11, when GDM debug is enabled, logs the user password when it contains invalid UTF8 encoded characters, which might allow local users to gain privileges by reading the information from syslog logs.	gnome	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00397034
9376	CVE-2010-2253	Medium		lwp-download in libwww-perl before 5.835 does not reject downloads to filenames that begin with a . (dot) character, which allows remote servers to create or overwrite files via (1) a 3xx redirect to a URL with a crafted filename or (2) a Content-Disposition header that suggests a crafted filename, and possibly execute arbitrary code as a consequence of writing to a dotfile in a home directory.	search.cpan libwww-perl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00224441
9377	CVE-2010-2252	Medium		GNU Wget 1.12 and earlier uses a server-provided filename instead of the original URL to determine the destination filename of a download, which allows remote servers to create or overwrite arbitrary files via a 3xx redirect to a URL with a .wgetrc filename followed by a 3xx redirect to a URL with a crafted filename, and possibly execute arbitrary code as a consequence of writing to a dotfile in a home directory.	wget.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00211679
9378	CVE-2010-2249	Medium		Memory leak in pngrutil.c in libpng before 1.2.44, and 1.4.x before 1.4.3, allows remote attackers to cause a denial of service (memory consumption and application crash) via a PNG image containing malformed Physical Scale (aka sCAL) chunks.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00220601
9379	CVE-2010-2248	High		fs/cifs/cifssmb.c in the CIFS implementation in the Linux kernel before 2.6.34-rc4 allows remote attackers to cause a denial of service (panic) via an SMB response packet with an invalid CountHigh value, as demonstrated by a response from an OS/2 server, related to the CIFSSMBWrite and CIFSSMBWrite2 functions.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00220599
9380	CVE-2010-2242	Low		Red Hat libvirt 0.2.0 through 0.8.2 creates iptables rules with improper mappings of privileged source ports, which allows guest OS users to bypass intended access restrictions by leveraging IP address and source-port values, as demonstrated by copying and deleting an NFS directory tree.	libvirt.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221113
9381	CVE-2010-2240	High		The do_anonymous_page function in mm/memory.c in the Linux kernel before 2.6.27.52, 2.6.32.x before 2.6.32.19, 2.6.34.x before 2.6.34.4, and 2.6.35.x before 2.6.35.2 does not properly separate the stack and the heap, which allows context-dependent attackers to execute arbitrary code by writing to the bottom page of a shared memory segment, as demonstrated by a memory-exhaustion attack against the X.Org X server.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00220092
9382	CVE-2010-2239	Medium		Red Hat libvirt, possibly 0.6.0 through 0.8.2, creates new images without setting the user-defined backing-store format, which allows guest OS users to read arbitrary files on the host OS via unspecified vectors.	libvirt.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221112
9383	CVE-2010-2238	Medium		Red Hat libvirt, possibly 0.7.2 through 0.8.2, recurses into disk-image backing stores without extracting the defined disk backing-store format, which might allow guest OS users to read arbitrary files on the host OS, and possibly have unspecified other impact, via unknown vectors.	libvirt.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221111
9384	CVE-2010-2237	Medium		Red Hat libvirt, possibly 0.6.1 through 0.8.2, looks up disk backing stores without referring to the user-defined main disk format, which might allow guest OS users to read arbitrary files on the host OS, and possibly have unspecified other impact, via unknown vectors.	libvirt.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00221110
9385	CVE-2010-2233	High		tif_getimage.c in LibTIFF 3.9.0 and 3.9.2 on 64-bit platforms, as used in ImageMagick, does not properly perform vertical flips, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted TIFF image, related to downsampled OJPEG input.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00220099
9386	CVE-2010-2226	Low		The xfs_swapext function in fs/xfs/xfs_dfrag.c in the Linux kernel before 2.6.35 does not properly check the file descriptors passed to the SWAPEXT ioctl, which allows local users to leverage write access and obtain read access by swapping one file into another file.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218773
9387	CVE-2010-2225	High		Use-after-free vulnerability in the SplObjectStorage unserializer in PHP 5.2.x and 5.3.x through 5.3.2 allows remote attackers to execute arbitrary code or obtain sensitive information via serialized data, related to the PHP unserialize function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325987
9388	CVE-2010-2199	High		lib/fsm.c in RPM 4.8.0 and earlier does not properly reset the metadata of an executable file during replacement of the file in an RPM package upgrade or deletion of the file in an RPM package removal, which might allow local users to bypass intended access restrictions by creating a hard link to a vulnerable file that has a POSIX ACL, a related issue to CVE-2010-2059.	rpm.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218813
9389	CVE-2010-2198	High		lib/fsm.c in RPM 4.8.0 and earlier does not properly reset the metadata of an executable file during replacement of the file in an RPM package upgrade or deletion of the file in an RPM package removal, which might allow local users to gain privileges or bypass intended access restrictions by creating a hard link to a vulnerable file that has (1) POSIX file capabilities or (2) SELinux context information, a related issue to CVE-2010-2059.	rpm.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00215699
9390	CVE-2010-2197	Medium		rpmbuild in RPM 4.8.0 and earlier does not properly parse the syntax of spec files, which allows user-assisted remote attackers to remove home directories via vectors involving a ;~ (semicolon tilde) sequence in a Name tag.	rpm.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218811

	A	B	C	D	E	F	G	H	I	J	K	L	M
9391	CVE-2010-2191	Medium		The (1) parse_str, (2) preg_match, (3) unpack, and (4) pack functions; the (5) ZEND_FETCH_RW, (6) ZEND_CONCAT, and (7) ZEND_ASSIGN_CONCAT opcodes; and the (8) ArrayObject::uasort method in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal function or handler. NOTE: vectors 2 through 4 are related to the call time pass by reference feature.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325989
9392	CVE-2010-2190	Medium		The (1) trim, (2) ltrim, (3) rtrim, and (4) substr_replace functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326004
9393	CVE-2010-2156	Medium		ISC DHCP 4.1 before 4.1.1-P1 and 4.0 before 4.0.2-P1 allows remote attackers to cause a denial of service (server exit) via a zero-length client ID.	isc dhcp.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218814
9394	CVE-2010-2101	Medium		The (1) strip_tags, (2) setcookie, (3) strtok, (4) wordwrap, (5) str_word_count, and (6) str_pad functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326004
9395	CVE-2010-2100	Medium		The (1) htmlentities, (2) htmlspecialchars, (3) str_getcsv, (4) http_build_query, (5) strpbrk, and (6) strtr functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326004
9396	CVE-2010-2097	Medium		The (1) iconv_mime_decode, (2) iconv_substr, and (3) iconv_mime_encode functions in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326004
9397	CVE-2010-2094	Medium		Multiple format string vulnerabilities in the phar extension in PHP 5.3 before 5.3.2 allow context-dependent attackers to obtain sensitive information (memory contents) and possibly execute arbitrary code via a crafted phar:// URI that is not properly handled by the (1) phar_stream_flush, (2) phar_wrapper_unlink, (3) phar_parse_url, or (4) phar_wrapper_open_url functions in ext/phar/stream.c; and the (5) phar_wrapper_open_dir function in ext/phar/dirstream.c, which triggers errors in the php_stream_wrapper_log_error function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325997
9398	CVE-2010-2093	Medium		Use-after-free vulnerability in the request shutdown functionality in PHP 5.2 before 5.2.13 and 5.3 before 5.3.2 allows context-dependent attackers to cause a denial of service (crash) via a stream context structure that is freed before destruction occurs.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325998
9399	CVE-2010-2089	Medium		The audioop module in Python 2.7 and 3.2 does not verify the relationships between size arguments and byte string lengths, which allows context-dependent attackers to cause a denial of service (memory corruption and application crash) via crafted arguments, as demonstrated by a call to audioop.reverse with a one-byte string, a different vulnerability than CVE-2010-1634.	Python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00217144
9400	CVE-2010-2074	Medium		istream.c in w3m 0.5.2 and possibly other versions, when ssl_verify_server is enabled, does not properly handle a '\0' character in a domain name in the (1) subject's Common Name or (2) Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	w3m.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218123
9401	CVE-2010-2071	Medium		The btrfs_xattr_set_acl function in fs/btrfs/acl.c in btrfs in the Linux kernel 2.6.34 and earlier does not check file ownership before setting an ACL, which allows local users to bypass file permissions by setting arbitrary ACLs, as demonstrated using setfacl.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218115
9402	CVE-2010-2068	Medium		mod_proxy_http.c in mod_proxy_http in the Apache HTTP Server 2.2.9 through 2.2.15, 2.3.4-alpha, and 2.3.5-alpha on Windows, NetWare, and OS/2, in certain configurations involving proxy worker pools, does not properly detect timeouts, which allows remote attackers to obtain a potentially sensitive response intended for a different client in opportunistic circumstances via a normal HTTP request.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00222220
9403	CVE-2010-2067	Medium		Stack-based buffer overflow in the TIFFFetchSubjectDistance function in tif_dirread.c in LibTIFF before 3.9.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long EXIF SubjectDistance field in a TIFF file.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218106
9404	CVE-2010-2066	Low		The mext_check_arguments function in fs/ext4/move_extent.c in the Linux kernel before 2.6.35 allows local users to overwrite an append-only file via a MOVE_EXT ioctl call that specifies this file as a donor.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218108
9405	CVE-2010-2065	Medium		Integer overflow in the TIFFroundup macro in LibTIFF before 3.9.3 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted TIFF file that triggers a buffer overflow.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218130
9406	CVE-2010-2064			rpcbind 0.2.0 allows local users to write to arbitrary files or gain privileges via a symlink attack on (1) /tmp/portmap.xdr and (2) /tmp/rpcbind.xdr.	rpcbind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1018-5181

	A	B	C	D	E	F	G	H	I	J	K	L	M
9407	CVE-2010-2063	High		Buffer overflow in the SMB1 packet chaining implementation in the chain_reply function in process.c in smbd in Samba 3.0.x before 3.3.13 allows remote attackers to cause a denial of service (memory corruption and daemon crash) or possibly execute arbitrary code via a crafted field in a packet.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218112
9408	CVE-2010-2061			rpcbind 0.2.0 does not properly validate (1) /tmp/portmap.xdr and (2) /tmp/rpcbind.xdr, which can be created by an attacker before the daemon is started.	rpcbind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Investigate	LIN1018-5182
9409	CVE-2010-2059	High		lib/fsm.c in RPM 4.8.0 and unspecified 4.7.x and 4.6.x versions, and RPM before 4.4.3, does not properly reset the metadata of an executable file during replacement of the file in an RPM package upgrade, which might allow local users to gain privileges by creating a hard link to a vulnerable (1) setuid or (2) setgid file.	rpm.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00215699
9410	CVE-2010-2055	High		Ghostscript 8.71 and earlier reads initialization files from the current working directory, which allows local users to execute arbitrary PostScript commands via a Trojan horse file, related to improper support for the -P- option to the gs program.	The PATCH for it is GPLv3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00226501
9411	CVE-2010-2008	Low		MySQL before 5.1.48 allows remote authenticated users with alter database privileges to cause a denial of service (server crash and database loss) via an ALTER DATABASE command with a #mysql50# string followed by a . (dot), .. (dot dot), ../ (dot dot slash) or similar sequence, and an UPGRADE DATA DIRECTORY NAME command, which causes MySQL to move certain directories to the server data directory.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00224440
9412	CVE-2010-1975	Medium		PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, and 8.4 before 8.4.4 does not properly check privileges during certain RESET ALL operations, which allows remote authenticated users to remove arbitrary parameter settings via a (1) ALTER USER or (2) ALTER DATABASE statement.	Postgresql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00217142
9413	CVE-2010-1974	Medium		Multiple unspecified vulnerabilities in the Safe (aka Safe.pm) module before 2.25 for Perl allow context-dependent attackers to inject and execute arbitrary code via vectors related to automagic methods. NOTE: this might overlap CVE-2010-1169 or CVE-2010-1447.	Perl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00217145
9414	CVE-2010-1917	Medium		Stack consumption vulnerability in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to cause a denial of service (PHP crash) via a crafted first argument to the fnmatch function, as demonstrated using a long string.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00325999
9415	CVE-2010-1915	Medium		The preg_quote function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature, modification of ZVALs whose values are not updated in the associated local variables, and access of previously-freed memory.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326004
9416	CVE-2010-1914	Medium		The Zend Engine in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information by interrupting the handler for the (1) ZEND_BW_XOR opcode (shift_left_function), (2) ZEND_SL opcode (bitwise_xor_function), or (3) ZEND_SR opcode (shift_right_function), related to the convert_to_long_base function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326001
9417	CVE-2010-1869	High		Stack-based buffer overflow in the parser function in GhostScript 8.70 and 8.64 allows context-dependent attackers to execute arbitrary code via a crafted PostScript file.	The PATCH for it is GPLv3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223173
9418	CVE-2010-1868	High		The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326002
9419	CVE-2010-1866	High		The dechunk filter in PHP 5.3 through 5.3.2, when decoding an HTTP chunked encoding stream, allows context-dependent attackers to cause a denial of service (crash) and possibly trigger memory corruption via a negative chunk size, which bypasses a signed comparison, related to an integer overflow in the chunk size decoder.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326003
9420	CVE-2010-1864	Medium		The addcslashes function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326004
9421	CVE-2010-1862	Medium		The chunk_split function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) by causing a userspace interruption of an internal function, related to the call time pass by reference feature.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326004
9422	CVE-2010-1861	Medium		The sysvshm extension for PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to write to arbitrary memory addresses by using an object's __sleep function to interrupt an internal call to the shm_put_var function, which triggers access of a freed resource.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326006
9423	CVE-2010-1860	Medium		The html_entity_decode function in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allows context-dependent attackers to obtain sensitive information (memory contents) or trigger memory corruption by causing a userspace interruption of an internal call, related to the call time pass by reference feature.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326004

	A	B	C	D	E	F	G	H	I	J	K	L	M
9424	CVE-2010-1850	Medium		Buffer overflow in MySQL 5.0 through 5.0.91 and 5.1 before 5.1.47 allows remote authenticated users to execute arbitrary code via a COM_FIELD_LIST command with a long table name.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218808
9425	CVE-2010-1849	Medium		The my_net_skip_rest function in sql/net_serv.cc in MySQL 5.0 through 5.0.91 and 5.1 before 5.1.47 allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by sending a large number of packets that exceed the maximum length.Per: http://cwe.mitre.org/data/definitions/371.html 'CWE-371: State Issues'	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218806
9426	CVE-2010-1848	Medium		Directory traversal vulnerability in MySQL 5.0 through 5.0.91 and 5.1 before 5.1.47 allows remote authenticated users to bypass intended table grants to read field definitions of arbitrary tables, and on 5.1 to read or delete content of arbitrary tables, via a .. (dot dot) in a table name.	mysql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218807
9427	CVE-2010-1797	High		Multiple stack-based buffer overflows in the cff_decoder_parse_charstrings function in the CFF Type2 CharStrings interpreter in cff/cffgload.c in FreeType before 2.4.2, as used in Apple iOS before 4.0.2 on the iPhone and iPod touch and before 3.2.2 on the iPad, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted CFF opcodes in embedded fonts in a PDF document, as demonstrated by JailbreakMe. NOTE: some of these details are obtained from third party information.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00226495
9428	CVE-2010-1675	Medium		bgpd in Quagga before 0.99.18 allows remote attackers to cause a denial of service (session reset) via a malformed AS_PATHLIMIT path attribute.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266367
9429	CVE-2010-1674	Medium		The extended-community parser in bgpd in Quagga before 0.99.18 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a malformed Extended Communities attribute.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266368
9430	CVE-2010-1666	Medium		Buffer overflow in Dan Pascu python-cjson 1.0.5, when UCS-4 encoding is enabled, allows context-dependent attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors involving crafted Unicode input to the cjson.encode function.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00216645
9431	CVE-2010-1646	Medium		The secure path feature in env.c in sudo 1.3.1 through 1.6.9p22 and 1.7.0 through 1.7.2p6 does not properly handle an environment that contains multiple PATH variables, which might allow local users to gain privileges via a crafted value of the last PATH variable.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00215250
9432	CVE-2010-1643	Medium		mm/shmem.c in the Linux kernel before 2.6.28-rc3, when strict overcommit is enabled, does not properly handle the export of shmemfs objects by knfsd, which allows attackers to cause a denial of service (NULL pointer dereference and knfsd crash) or possibly have unspecified other impact via unknown vectors.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00214457
9433	CVE-2010-1642	Medium		The reply_sesssetup_and_X_spnego function in sesssetup.c in smbd in Samba before 3.4.8 and 3.5.x before 3.5.2 allows remote attackers to trigger an out-of-bounds read, and cause a denial of service (process crash), via a \xff\xff security blob length in a Session Setup AndX request.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00214223
9434	CVE-2010-1641	Medium		The do_gfs2_set_flags function in fs/gfs2/file.c in the Linux kernel before 2.6.34-git10 does not verify the ownership of a file, which allows local users to bypass intended access restrictions via a SETFLAGS ioctl request.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00214222
9435	CVE-2010-1636	Low		The btrfs_ioctl_clone function in fs/btrfs/ioctl.c in the btrfs functionality in the Linux kernel 2.6.29 through 2.6.32, and possibly other versions, does not ensure that a cloned file descriptor has been opened for reading, which allows local users to read sensitive information from a write-only file descriptor.	Linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00213659
9436	CVE-2010-1635	Medium		The chain_reply function in process.c in smbd in Samba before 3.4.8 and 3.5.x before 3.5.2 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash) via a Negotiate Protocol request with a certain 0x0003 field value followed by a Session Setup AndX request with a certain 0x8003 field value.Per: http://cwe.mitre.org/data/definitions/476.html 'NULL Pointer Dereference'	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00214225
9437	CVE-2010-1634	Medium		Multiple integer overflows in audioop.c in the audioop module in Python 2.6, 2.7, 3.1, and 3.2 allow context-dependent attackers to cause a denial of service (application crash) via a large fragment, as demonstrated by a call to audioop.lin2lin with a long string in the first argument, leading to a buffer overflow. NOTE: this vulnerability exists because of an incorrect fix for CVE-2008-3143.5.	Python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00217141
9438	CVE-2010-1633	Medium		RSA verification recovery in the EVP_PKEY_verify_recover function in OpenSSL 1.x before 1.0.0a, as used by pkeyutl and possibly other applications, returns uninitialized memory upon failure, which might allow context-dependent attackers to bypass intended key requirements or obtain sensitive information via unspecified vectors. NOTE: some of these details are obtained from third party information.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218815
9439	CVE-2010-1626	Medium		MySQL before 5.1.46 allows local users to delete the data and index files of another user's MyISAM table via a symlink attack in conjunction with the DROP TABLE command, a different vulnerability than CVE-2008-4098 and CVE-2008-7247.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00213658

	A	B	C	D	E	F	G	H	I	J	K	L	M
9440	CVE-2010-1623	Medium		The apr_brigade_split_line function in buckets/apr_brigade.c in the Apache Portable Runtime Utility library (aka APR-util) before 1.3.10, as used in the mod_reqtimeout module in the Apache HTTP Server and other software, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors.	Apache.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237158
9441	CVE-2010-1621	Medium		The mysql_uninstall_plugin function in sql/sql_plugin.cc in MySQL before 5.1.46 does not check privileges before uninstalling a plugin, which allows remote attackers to uninstall arbitrary plugins via the UNINSTALL PLUGIN command.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00211420
9442	CVE-2010-1488	Low		The proc_oom_score function in fs/proc/base.c in the Linux kernel before 2.6.34-rc4 uses inappropriate data structures during selection of a candidate for the OOM killer, which might allow local users to cause a denial of service via unspecified patterns of task creation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00209260
9443	CVE-2010-1452	Medium		The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00226494
9444	CVE-2010-1451	Medium		The TSB I-TLB load implementation in arch/sparc/kernel/tsb.S in the Linux kernel before 2.6.33 on the SPARC platform does not properly obtain the value of a certain _PAGE_EXEC_4U bit and consequently does not properly implement a non-executable stack, which makes it easier for context-dependent attackers to exploit stack-based buffer overflows via a crafted application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00211419
9445	CVE-2010-1450	High		Multiple buffer overflows in the RLE decoder in the rgbimg module in Python 2.5 allow remote attackers to have an unspecified impact via an image file containing crafted data that triggers improper processing within the (1) longimagedata or (2) expandrow function.	Python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00211613
9446	CVE-2010-1449	High		Integer overflow in rgbimgmodule.c in the rgbimg module in Python 2.5 allows remote attackers to have an unspecified impact via a large image that triggers a buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-3143.12.	Python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00211614
9447	CVE-2010-1447	High		PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 does not properly restrict PL/perl procedures, which might allow remote attackers to execute arbitrary Perl code via a crafted script, related to the Safe module (aka Safe.pm) for Perl.	Postgresql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00212021
9448	CVE-2010-1446	Low		arch/powerpc/mm/fsl_booke_mmu.c in KGDB in the Linux kernel 2.6.30 and other versions before 2.6.33, when running on PowerPC, does not properly perform a security check for access to a kernel page, which allows local users to overwrite arbitrary kernel memory, related to Fsl booke.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202644
9449	CVE-2010-1437	Low		Race condition in the find_keyring_by_name function in security/keys/keyring.c in the Linux kernel 2.6.34-rc5 and earlier allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact via keyctl session commands that trigger access to a dead keyring that is undergoing deletion by the key_cleanup function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00209842
9450	CVE-2010-1436	Medium		gfs2 in the Linux kernel 2.6.18, and possibly other versions, does not properly handle when the gfs2_quota struct occupies two separate pages, which allows local users to cause a denial of service (kernel panic) via certain manipulations that cause an out-of-bounds write, as demonstrated by writing from an ext3 file system to a gfs2 file system.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00209841
9451	CVE-2010-1411	Medium		Multiple integer overflows in the Fax3SetupState function in tif_fax3.c in the FAX3 decoder in LibTIFF before 3.9.3, as used in ImageIO in Apple Mac OS X 10.5.8 and Mac OS X 10.6 before 10.6.4, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted TIFF file that triggers a heap-based buffer overflow.	Libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00212513
9452	CVE-2010-1330	Medium		The regular expression engine in JRuby before 1.4.1, when $KCODE is set to 'u', does not properly handle characters immediately after a UTF-8 character, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted string.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00392076
9453	CVE-2010-1324	Medium		MIT Kerberos 5 (aka krb5) 1.7.x and 1.8.x through 1.8.3 does not properly determine the acceptability of checksums, which might allow remote attackers to forge GSS tokens, gain privileges, or have unspecified other impact via (1) an unkeyed checksum, (2) an unkeyed PAC checksum, or (3) a KrbFastArmoredReq checksum based on an RC4 key.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247365
9454	CVE-2010-1322	Medium		The merge_authdata function in kdc_authdata.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.8.x before 1.8.4 does not properly manage an index into an authorization-data list, which allows remote attackers to cause a denial of service (daemon crash), or possibly obtain sensitive information, spoof authorization, or execute arbitrary code, via a TGS request, as demonstrated by a request from a Windows Active Directory client.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234375

	A	B	C	D	E	F	G	H	I	J	K	L	M
9455	CVE-2010-1321	Medium		The kg_accept_krb5 function in krb5/accept_sec_context.c in the GSS-API library in MIT Kerberos 5 (aka krb5) through 1.7.1 and 1.8 before 1.8.2, as used in kadmind and other applications, does not properly check for invalid GSS-API tokens, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via an AP-REQ message in which the authenticator's checksum field is missing.Per: http://cwe.mitre.org/data/definitions/476.html CWE-476: NULL Pointer Dereference'	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00210809
9456	CVE-2010-1320	Medium		Double free vulnerability in do_tgs_req.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.7.x and 1.8.x before 1.8.2 allows remote authenticated users to cause a denial of service (daemon crash) or possibly execute arbitrary code via a request associated with (1) renewal or (2) validation.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00209225
9457	CVE-2010-1205	High		Buffer overflow in pngpread.c in libpng before 1.2.44 and 1.4.x before 1.4.3, as used in progressive applications, might allow remote attackers to execute arbitrary code via a PNG image that triggers an additional data row.	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00222224
9458	CVE-2010-1188	High		Use-after-free vulnerability in net/ipv4/tcp_input.c in the Linux kernel 2.6 before 2.6.20, when IPV6_RECVPKTINFO is set on a listening socket, allows remote attackers to cause a denial of service (kernel panic) via a SYN packet while the socket is in a listening (TCP_LISTEN) state, which is not properly handled causes the skb structure to be freed.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00205471
9459	CVE-2010-1187	Medium		The Transparent Inter-Process Communication (TIPC) functionality in Linux kernel 2.6.33, and possibly other versions, allows local users to cause a denial of service (kernel OOPS) by sending datagrams through AF_TIPC before entering network mode, which triggers a NULL pointer dereference.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00205613
9460	CVE-2010-1173	High		The sctp_process_unk_param function in net/sctp/sm_make_chunk.c in the Linux kernel 2.6.33.3 and earlier, when SCTP is enabled, allows remote attackers to cause a denial of service (system crash) via an SCTPChunkInit packet containing multiple invalid parameters that require a large amount of error data.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00207927
9461	CVE-2010-1172	Low		DBus-GLib 0.73 disregards the access flag of exported GObject properties, which allows local users to bypass intended access restrictions and possibly cause a denial of service by modifying properties, as demonstrated by properties of the (1) DeviceKit-Power, (2) NetworkManager, and (3) ModemManager services.	dbus-glib.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00227461
9462	CVE-2010-1170	Medium		The PL/Tcl implementation in PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 loads Tcl code from the pltcl_modules table regardless of the table's ownership and permissions, which allows remote authenticated users, with database-creation privileges, to execute arbitrary Tcl code by creating this table and inserting a crafted Tcl script.	Postgresql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00212023
9463	CVE-2010-1169	High		PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 does not properly restrict PL/perl procedures, which allows remote authenticated users, with database-creation privileges, to execute arbitrary Perl code via a crafted script, related to the Safe module (aka Safe.pm) for Perl.	Postgresql.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00212022
9464	CVE-2010-1168	High		The Safe (aka Safe.pm) module before 2.25 for Perl allows context-dependent attackers to bypass intended (1) Safe::reval and (2) Safe::rdo access restrictions, and inject and execute arbitrary code, via vectors involving implicitly called methods and implicitly blessed objects, as demonstrated by the (a) DESTROY and (b) AUTOLOAD methods, related to automagic methods.	Perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00212020
9465	CVE-2010-1166	High		The fbComposite function in fbpict.c in the Render extension in the X server in X.Org X11R7.1 allows remote authenticated users to cause a denial of service (memory corruption and daemon crash) or possibly execute arbitrary code via a crafted request, related to an incorrect macro definition.	xorg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00211189
9466	CVE-2010-1163	Medium		The command matching functionality in sudo 1.6.8 through 1.7.2p5 does not properly handle when a file in the current working directory has the same name as a pseudo-command in the sudoers file and the PATH contains an entry for ., which allows local users to execute arbitrary commands via a Trojan horse executable, as demonstrated using sudoedit, a different vulnerability than CVE-2010-0426.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00209244
9467	CVE-2010-1162	High		The release_one_tty function in drivers/char/tty_io.c in the Linux kernel before 2.6.34-rc4 omits certain required calls to the put_pid function, which has unspecified impact and local attack vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00209243
9468	CVE-2010-1158	Medium		Integer overflow in the regular expression engine in Perl 5.8.x allows context-dependent attackers to cause a denial of service (stack consumption and application crash) by matching a crafted regular expression against a long string.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00209223
9469	CVE-2010-1151	Medium		Race condition in the mod_auth_shadow module for the Apache HTTP Server allows remote attackers to bypass authentication, and read and possibly modify data, via vectors related to improper interaction with an external helper application for validation of credentials.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00206925

	A	B	C	D	E	F	G	H	I	J	K	L	M
9470	CVE-2010-1148	Medium		The cifs_create function in fs/cifs/dir.c in the Linux kernel 2.6.33.2 and earlier allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a NULL nameidata (aka nd) field in a POSIX file-creation request to a server that supports UNIX extensions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00206236
9471	CVE-2010-1146	Medium		The Linux kernel 2.6.33.2 and earlier, when a ReiserFS filesystem exists, does not restrict read or write access to the .reiserfs_priv directory, which allows local users to gain privileges by modifying (1) extended attributes or (2) ACLs, as demonstrated by deleting a file under .reiserfs_priv/xattrs/.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00206237
9472	CVE-2010-1088	Medium		fs/namei.c in Linux kernel 2.6.18 through 2.6.34 does not always follow NFS automount symlinks, which allows attackers to have an unknown impact, related to LOOKUP_FOLLOW.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204850
9473	CVE-2010-1087	High		The nfs_wait_on_request function in fs/nfs/pagelist.c in Linux kernel 2.6.x through 2.6.33-rc5 allows attackers to cause a denial of service (Oops) via unknown vectors related to truncating a file and an operation that is not interruptible.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204852
9474	CVE-2010-1086	High		The ULE decapsulation functionality in drivers/media/dvb/dvb-core/dvb_net.c in dvb-core in Linux kernel 2.6.33 and earlier allows attackers to cause a denial of service (infinite loop) via a crafted MPEG2-TS frame, related to an invalid Payload Pointer ULE.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204851
9475	CVE-2010-1085	High		The azx_position_ok function in hda_intel.c in Linux kernel 2.6.33-rc4 and earlier, when running on the AMD780V chip set, allows context-dependent attackers to cause a denial of service (crash) via unknown manipulations that trigger a divide-by-zero error.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204849
9476	CVE-2010-1084	High		Linux kernel 2.6.18 through 2.6.33, and possibly other versions, allows remote attackers to cause a denial of service (memory corruption) via a large number of Bluetooth sockets, related to the size of sysfs files in (1) net/bluetooth/l2cap.c, (2) net/bluetooth/rfcomm/core.c, (3) net/bluetooth/rfcomm/sock.c, and (4) net/bluetooth/sco.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204857
9477	CVE-2010-1083	Medium		The processcompl_compat function in drivers/usb/core/devio.c in Linux kernel 2.6.x through 2.6.32, and possibly other versions, does not clear the transfer buffer before returning to userspace when a USB command fails, which might make it easier for physically proximate attackers to obtain sensitive information (kernel memory).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204848
9478	CVE-2010-0928	Medium		OpenSSL 0.9.8i on the Gaisler Research LEON3 SoC on the Xilinx Virtex-II Pro FPGA uses a Fixed Width Exponentiation (FWE) algorithm for certain signature calculations, and does not verify the signature before providing it to a caller, which makes it easier for physically proximate attackers to determine the private key via a modified supply voltage for the microprocessor, related to a fault-based attack.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204145
9479	CVE-2010-0926	Low		The default configuration of smbd in Samba before 3.3.11, 3.4.x before 3.4.6, and 3.5.x before 3.5.0rc3, when a writable share exists, allows remote authenticated users to leverage a directory traversal vulnerability, and access arbitrary files, by using the symlink command in smbclient to create a symlink containing ... (dot dot) sequences, related to the combination of the unix extensions and wide links options.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202824
9480	CVE-2010-0832	Medium		pam_motd (aka the MOTD module) in libpam-modules before 1.1.0-2ubuntu1.1 in PAM on Ubuntu 9.10 and libpam-modules before 1.1.1-2ubuntu5 in PAM on Ubuntu 10.04 LTS allows local users to change the ownership of arbitrary files via a symlink attack on .cache in a user's home directory, related to user file stamps and the motd.legal-notice file.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00224437
9481	CVE-2010-0830	Medium		Integer signedness error in the elf_get_dynamic_info function in elf/dynamic-link.h in ld.so in the GNU C Library (aka glibc or libc6) 2.0.1 through 2.11.1, when the --verify option is used, allows user-assisted remote attackers to execute arbitrary code via a crafted ELF program with a negative value for a certain d_tag structure member in the ELF header.	gnu glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218802
9482	CVE-2010-0789	Low		fusermount in FUSE before 2.7.5, and 2.8.x before 2.8.2, allows local users to unmount an arbitrary FUSE filesystem share via a symlink attack on a mountpoint.	fuse	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202795
9483	CVE-2010-0787	Medium		client/mount.cifs.c in mount.cifs in smbfs in Samba 3.0.22, 3.0.28a, 3.2.3, 3.3.2, 3.4.0, and 3.4.5 allows local users to mount a CIFS share on an arbitrary mountpoint, and gain privileges, via a symlink attack on the mountpoint directory file.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202794
9484	CVE-2010-0743	Medium		Multiple format string vulnerabilities in isns.c in (1) Linux SCSI target framework (aka tgt or scsi-target-utils) 1.0.3, 0.9.5, and earlier and (2) iSCSI Enterprise Target (aka iscsitarget) 0.4.16 allow remote attackers to cause a denial of service (tgtd daemon crash) or possibly have unspecified other impact via vectors that involve the isns_attr_query and qry_rsp_handle functions, and are related to (a) client appearance and (b) client disappearance messages.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00209424
9485	CVE-2010-0742	High		The Cryptographic Message Syntax (CMS) implementation in crypto/cms/cms_asn1.c in OpenSSL before 0.9.8o and 1.x before 1.0.0a does not properly handle structures that contain OriginatorInfo, which allows context-dependent attackers to modify invalid memory locations or conduct double-free attacks, and possibly execute arbitrary code, via unspecified vectors.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218812

	A	B	C	D	E	F	G	H	I	J	K	L	M
9486	CVE-2010-0741	Medium		The virtio_net_bad_features function in hw/virtio-net.c in the virtio-net driver in the Linux kernel before 2.6.26, when used on a guest OS in conjunction with qemu-kvm 0.11.0 or KVM 83, allows remote attackers to cause a denial of service (guest OS crash, and an associated qemu-kvm process exit) by sending a large amount of network traffic to a TCP port on the guest OS, related to a virtio-net whitelist that includes an improper implementation of TCP Segment Offloading (TSO).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00205472
9487	CVE-2010-0740	Medium		The ssl3_get_record function in ssl/s3_pkt.c in OpenSSL 0.9.8f through 0.9.8m allows remote attackers to cause a denial of service (crash) via a malformed record in a TLS connection that triggers a NULL pointer dereference, related to the minor version number. NOTE: some of these details are obtained from third party information.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00206486
9488	CVE-2010-0734	Medium		content_encoding.c in libcurl 7.10.5 through 7.19.7, when zlib is enabled, does not properly restrict the amount of callback data sent to an application that requests automatic decompression, which might allow remote attackers to cause a denial of service (application crash) or have unspecified other impact by sending crafted compressed data to an application that relies on the intended data-length limit.	libcurl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204095
9489	CVE-2010-0733	Low		Integer overflow in src/backend/executor/nodeHash.c in PostgreSQL 8.4.1 and earlier, and 8.5 through 8.5alpha2, allows remote authenticated users to cause a denial of service (daemon crash) via a SELECT statement with many LEFT JOIN clauses, related to certain hashtable size calculations.	PostgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204094
9490	CVE-2010-0732	Medium		gdk/gdkwindow.c in GTK+ before 2.18.5, as used in gnome-screensaver before 2.28.1, performs implicit paints on windows of type GDK_WINDOW_FOREIGN, which triggers an X error in certain circumstances and consequently allows physically proximate attackers to bypass screen locking and access an unattended workstation by pressing the Enter key many times.	gtk	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00206484
9491	CVE-2010-0731	High		The gnutls_x509_crt_get_serial function in the GnuTLS library before 1.2.1, when running on big-endian, 64-bit platforms, calls the asn1_read_value with a pointer to the wrong data type and the wrong length value, which allows remote attackers to bypass the certificate revocation list (CRL) check and cause a stack-based buffer overflow via a crafted X.509 certificate, related to extraction of a serial number.	GnuTLS	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00203844
9492	CVE-2010-0729	Medium		A certain Red Hat patch for the Linux kernel in Red Hat Enterprise Linux (RHEL) 4 on the ia64 platform allows local users to use ptrace on an arbitrary process, and consequently gain privileges, via vectors related to a missing ptrace_check_attach call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00203634
9493	CVE-2010-0728	High		smbd in Samba 3.3.11, 3.4.6, and 3.5.0, when libcap support is enabled, runs with the CAP_DAC_OVERRIDE capability, which allows remote authenticated users to bypass intended file permissions via standard filesystem operations with any client.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204142
9494	CVE-2010-0727	Medium		The gfs2_lock function in the Linux kernel before 2.6.34-rc1-next-20100312, and the gfs_lock function in the Linux kernel on Red Hat Enterprise Linux (RHEL) 5 and 6, does not properly remove POSIX locks on files that are setgid without group-execute permission, which allows local users to cause a denial of service (BUG and system crash) by locking a file on a (1) GFS or (2) GFS2 filesystem, and then changing this file's permissions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00203631
9495	CVE-2010-0634	High		Unspecified vulnerability in Fast Lexical Analyzer Generator (flex) before 2.5.35 has unknown impact and attack vectors.	flex	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00200927
9496	CVE-2010-0629	Medium		Use-after-free vulnerability in kadmin/server/server_stubs.c in kadmind in MIT Kerberos 5 (aka krb5) 1.5 through 1.6.3 allows remote authenticated users to cause a denial of service (daemon crash) via a request from a kadmin client that sends an invalid API version number.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00205815
9497	CVE-2010-0628	Medium		The spnego_gss_accept_sec_context function in lib/gssapi/spnego/spnego_mech.c in the SPNEGO GSS-API functionality in MIT Kerberos 5 (aka krb5) 1.7 before 1.7.2 and 1.8 before 1.8.1 allows remote attackers to cause a denial of service (assertion failure and daemon crash) via an invalid packet that triggers incorrect preparation of an error token.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00203630
9498	CVE-2010-0624	High		Heap-based buffer overflow in the rmt_read__ function in lib/rtapelib.c in the rmt client functionality in GNU tar before 1.23 and GNU cpio before 2.11 allows remote rmt servers to cause a denial of service (memory corruption) or possibly execute arbitrary code by sending more data than was requested, related to archive filenames that contain a : (colon) character.	cpio tar	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00201715
9499	CVE-2010-0623	Low		The futex_lock_pi function in kernel/futex.c in the Linux kernel before 2.6.33-rc7 does not properly manage a certain reference count, which allows local users to cause a denial of service (OOPS) via vectors involving an unmount of an ext3 filesystem.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00200242
9500	CVE-2010-0622	Low		The wake_futex_pi function in kernel/futex.c in the Linux kernel before 2.6.33-rc7 does not properly handle certain unlock operations for a Priority Inheritance (PI) futex, which allows local users to cause a denial of service (OOPS) and possibly have unspecified other impact via vectors involving modification of the futex value from user space.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00200241

	A	B	C	D	E	F	G	H	I	J	K	L	M
9501	CVE-2010-0547	Low		client/mount.cifs.c in mount.cifs in smbfs in Samba 3.4.5 and earlier does not verify that the (1) device name and (2) mountpoint strings are composed of valid characters, which allows local users to cause a denial of service (mtab corruption) via a crafted string.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00200925
9502	CVE-2010-0542	Medium		The _WriteProlog function in texttops.c in texttops in the Text Filter subsystem in CUPS before 1.4.4 does not check the return values of certain calloc calls, which allows remote attackers to cause a denial of service (NULL pointer dereference or heap memory corruption) or possibly execute arbitrary code via a crafted file.	cups.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00222225
9503	CVE-2010-0540	Medium		Cross-site request forgery (CSRF) vulnerability in the web interface in CUPS before 1.4.4, as used on Apple Mac OS X 10.5.8, Mac OS X 10.6 before 10.6.4, and other platforms, allows remote attackers to hijack the authentication of administrators for requests that change settings.	CUPS	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218125
9504	CVE-2010-0442	Medium		The bitsubstr function in backend/utils/adt/varbit.c in PostgreSQL 8.0.23, 8.1.11, and 8.3.8 allows remote authenticated users to cause a denial of service (daemon crash) or have unspecified other impact via vectors involving a negative integer in the third argument, as demonstrated by a SELECT statement that contains a call to the substring function for a bit string, related to an overflow.	postgresql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00198026
9505	CVE-2010-0437	High		The ip6_dst_lookup_tail function in net/ipv6/ip6_output.c in the Linux kernel before 2.6.27 does not properly handle certain circumstances involving an IPv6 TUN network interface and a large number of neighbors, which allows attackers to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via unknown vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202822
9506	CVE-2010-0435	Medium		The Hypervisor (aka rhev-hypervisor) in Red Hat Enterprise Virtualization (RHEV) 2.2, and KVM 83, when the Intel VT-x extension is enabled, allows guest OS users to cause a denial of service (NULL pointer dereference and host OS crash) via vectors related to instruction emulation.Per: http://cwe.mitre.org/data/definitions/476.html 'NULL Pointer Dereference'	kvm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00227462
9507	CVE-2010-0434	Medium		The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204139
9508	CVE-2010-0433	Medium		The kssl_keytab_is_available function in ssl/kssl.c in OpenSSL before 0.9.8n, when Kerberos is enabled but Kerberos configuration files cannot be opened, does not check a certain return value, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via SSL cipher negotiation, as demonstrated by a chroot installation of Dovecot or stunnel without Kerberos configuration files inside the chroot.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202807
9509	CVE-2010-0431	Medium		QEMU-KVM, as used in the Hypervisor (aka rhev-hypervisor) in Red Hat Enterprise Virtualization (RHEV) 2.2 and KVM 83, does not properly validate guest QXL driver pointers, which allows guest OS users to cause a denial of service (invalid pointer dereference and guest OS crash) or possibly gain privileges via unspecified vectors.	kvm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232309
9510	CVE-2010-0430	High		libspice, as used in QEMU-KVM in Red Hat Enterprise Virtualization Hypervisor (aka RHEV-H or rhev-hypervisor) before 5.5-2.2 and possibly other products, allows guest OS users to read from or write to arbitrary QEMU memory by modifying the address that is used by Cairo for memory mappings.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-2522
9511	CVE-2010-0429	Medium		libspice, as used in QEMU-KVM in the Hypervisor (aka rhev-hypervisor) in Red Hat Enterprise Virtualization (RHEV) 2.2 and qspice 0.3.0, does not properly restrict the addresses upon which memory-management actions are performed, which allows guest OS users to cause a denial of service (guest OS crash) or possibly gain privileges via unspecified vectors.	kvm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232311
9512	CVE-2010-0428	Medium		libspice, as used in QEMU-KVM in the Hypervisor (aka rhev-hypervisor) in Red Hat Enterprise Virtualization (RHEV) 2.2 and qspice 0.3.0, does not properly validate guest QXL driver pointers, which allows guest OS users to cause a denial of service (invalid pointer dereference and guest OS crash) or possibly gain privileges via unspecified vectors.	kvm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232310
9513	CVE-2010-0427	Medium		sudo 1.6.x before 1.6.9p21, when the runas_default option is used, does not properly set group memberships, which allows local users to gain privileges via a sudo command.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00201563
9514	CVE-2010-0426	Medium		sudo 1.6.x before 1.6.9p21 and 1.7.x before 1.7.2p4, when a pseudo-command is enabled, permits a match between the name of the pseudo-command and the name of an executable file in an arbitrary directory, which allows local users to gain privileges via a crafted executable file, as demonstrated by a file named sudoedit in a user's home directory.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00201562
9515	CVE-2010-0425	High		modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.3.x before 2.3.7 on Windows does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which has unspecified impact and remote attack vectors related to orphaned callback pointers.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204140

	A	B	C	D	E	F	G	H	I	J	K	L	M
9516	CVE-2010-0424	Low		The edit_cmd function in crontab.c in (1) cronie before 1.4.4 and (2) Vixie cron (vixie-cron) allows local users to change the modification times of arbitrary files, and consequently cause a denial of service, via a symlink attack on a temporary file in the /tmp directory.	cron	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00200902
9517	CVE-2010-0421	Medium		Array index error in the hb_ot_layout_build_glyph_classes function in pango/opentype/hb-ot-layout.cc in Pango before 1.27.1 allows context-dependent attackers to cause a denial of service (application crash) via a crafted font file, related to building a synthetic Glyph Definition (aka GDEF) table by using this font's charmap and the Unicode property database.	Pango	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00203801
9518	CVE-2010-0419	Medium		The x86 emulator in KVM 83, when a guest is configured for Symmetric Multiprocessing (SMP), does not properly restrict writing of segment selectors to segment registers, which might allow guest OS users to cause a denial of service (guest OS crash) or gain privileges on the guest OS by leveraging access to a (1) IO port or (2) MMIO region, and replacing an instruction in between emulator entry and instruction fetch.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00201141
9519	CVE-2010-0415	Medium		The do_pages_move function in mm/migrate.c in the Linux kernel before 2.6.33-rc7 does not validate node values, which allows local users to read arbitrary kernel memory locations, cause a denial of service (OOPS), and possibly have unspecified other impact by specifying a node that is not part of the kernel's node set.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199758
9520	CVE-2010-0410	Medium		drivers/connector/connector.c in the Linux kernel before 2.6.32.8 allows local users to cause a denial of service (memory consumption and system crash) by sending the kernel many NETLINK_CONNECTOR messages.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199121
9521	CVE-2010-0408	Medium		The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.Per: http://cwe.mitre.org/data/definitions/703.html CWE-703: Failure to Handle Exceptional Conditions	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204143
9522	CVE-2010-0407	Medium		Multiple buffer overflows in the MSGFunctionDemarshall function in winscard_svc.c in the PC/SC Smart Card daemon (aka PCSCD) in MUSCLE PCSC-Lite before 1.5.4 allow local users to gain privileges via crafted message data, which is improperly demarshalled.	pcsc-lite.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00222223
9523	CVE-2010-0405	Medium		Integer overflow in the BZ2_decompress function in decompress.c in bzip2 and libbzip2 before 1.0.6 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted compressed file.	bzip2.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00230121
9524	CVE-2010-0397	Medium		The xmlrpc extension in PHP 5.3.1 does not properly handle a missing methodName element in the first argument to the xmlrpc_decode_request function, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) and possibly have unspecified other impact via a crafted argument.Per: http://cwe.mitre.org/data/slices/2000.html Improper Check for Unusual or Exceptional Conditions CWE-754	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326009
9525	CVE-2010-0382	High		ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta handles out-of-bailiwick data accompanying a secure response without re-fetching from the original source, which allows remote attackers to have an unspecified impact via a crafted response, aka Bug 20819. NOTE: this vulnerability exists because of a regression during the fix for CVE-2009-4022.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199177
9526	CVE-2010-0309	Medium		The pit_ioport_read function in the Programmable Interval Timer (PIT) emulation in i8254.c in KVM 83 does not properly use the pit_state data structure, which allows guest OS users to cause a denial of service (host OS crash or hang) by attempting to read the /dev/port file.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199116
9527	CVE-2010-0307	Medium		The load_elf_binary function in fs/binfmt_elf.c in the Linux kernel before 2.6.32.8 on the x86_64 platform does not ensure that the ELF interpreter is available before a call to the SET_PERSONALITY macro, which allows local users to cause a denial of service (system crash) via a 32-bit application that attempts to execute a 64-bit application and then triggers a segmentation fault, as demonstrated by amd64_killer, related to the flush_old_exec function.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00198661
9528	CVE-2010-0306	Medium		The x86 emulator in KVM 83, when a guest is configured for Symmetric Multiprocessing (SMP), does not use the Current Privilege Level (CPL) and I/O Privilege Level (IOPL) to restrict instruction execution, which allows guest OS users to cause a denial of service (guest OS crash) or gain privileges on the guest OS by leveraging access to a (1) IO port or (2) MMIO region, and replacing an instruction in between emulator entry and instruction fetch, a related issue to CVE-2010-0298.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199760
9529	CVE-2010-0299	Medium		openSUSE 11.2 installs the devtmpfs root directory with insecure permissions (1777), which allows local users to gain privileges via unspecified vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00198027

	A	B	C	D	E	F	G	H	I	J	K	L	M
9530	CVE-2010-0298	Medium		The x86 emulator in KVM 83 does not use the Current Privilege Level (CPL) and I/O Privilege Level (IOPL) in determining the memory access available to CPL3 code, which allows guest OS users to cause a denial of service (guest OS crash) or gain privileges on the guest OS by leveraging access to a (1) IO port or (2) MMIO region, a related issue to CVE-2010-0306.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199759
9531	CVE-2010-0297	Medium		Buffer overflow in the usb_host_handle_control function in the USB passthrough handling implementation in usb-linux.c in QEMU before 0.11.1 allows guest OS users to cause a denial of service (guest OS crash or hang) or possibly execute arbitrary code on the host OS via a crafted USB packet.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199115
9532	CVE-2010-0296	High		The encode_name macro in misc/mntent_r.c in the GNU C Library (aka glibc or libc6) 2.11.1 and earlier, as used by ncpmount and mount.cifs, does not properly handle newline characters in mountpoint names, which allows local users to cause a denial of service (mtab corruption), or possibly modify mount options and gain privileges, via a crafted mount request.	gnu glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00206452
9533	CVE-2010-0291	Medium		The Linux kernel before 2.6.32.4 allows local users to gain privileges or cause a denial of service (panic) by calling the (1) mmap or (2) mremap function, aka the do_mremap() mess or mremap/mmap mess.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197995
9534	CVE-2010-0290	Medium		Unspecified vulnerability in ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta, with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks by receiving a recursive client query and sending a response that contains (1) CNAME or (2) DNAME records, which do not have the intended validation before caching, aka Bug 20737. NOTE: this vulnerability exists because of an incomplete fix for CVE-2009-4022.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199177
9535	CVE-2010-0285	Low		gnome-screensaver 2.14.3, 2.22.2, 2.27.x, 2.28.0, and 2.28.3, when the X configuration enables the extend screen option, allows physically proximate attackers to bypass screen locking, access an unattended workstation, and view half of the GNOME desktop by attaching an external monitor.	WRLinux doesn't ship gnome screensaver.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197605
9536	CVE-2010-0283	High		The Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.7 before 1.7.2, and 1.8 alpha, allows remote attackers to cause a denial of service (assertion failure and daemon crash) via an invalid (1) AS-REQ or (2) TGS-REQ request.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202124
9537	CVE-2010-0218	Medium		ISC BIND 9.7.2 through 9.7.2-P1 uses an incorrect ACL to restrict the ability of Recursion Desired (RD) queries to access the cache, which allows remote attackers to obtain potentially sensitive information via a DNS query.	Isc bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00237159
9538	CVE-2010-0213	Low		BIND 9.7.1 and 9.7.1-P1, when a recursive validating server has a trust anchor that is configured statically or via DNSSEC Lookaside Validation (DLV), allows remote attackers to cause a denial of service (infinite loop) via a query for an RRSIG record whose answer is not in the cache, which causes BIND to repeatedly send RRSIG queries to the authoritative servers.	bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00226496
9539	CVE-2010-0212	Medium		OpenLDAP 2.4.22 allows remote attackers to cause a denial of service (crash) via a modrdn call with a zero-length RDN destination string, which is not properly handled by the smr_normalize function and triggers a NULL pointer dereference in the IASStringNormalize function in schema_init.c, as demonstrated using the Codenomicon LDAPv3 test suite.	openldap.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218116
9540	CVE-2010-0211	Medium		The slap_modrdn2mods function in modrdn.c in OpenLDAP 2.4.22 does not check the return value of a call to the smr_normalize function, which allows remote attackers to cause a denial of service (segmentation fault) and possibly execute arbitrary code via a modrdn call with an RDN string containing invalid UTF-8 sequences, which triggers a free of an invalid, uninitialized pointer in the slap_mods_free function, as demonstrated using the Codenomicon LDAPv3 test suite.	openldap.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218116
9541	CVE-2010-0205	High		The png_decompress_chunk function in pngrutil.c in libpng 1.0.x before 1.0.53, 1.2.x before 1.2.43, and 1.4.x before 1.4.1 does not properly handle compressed ancillary-chunk data that has a disproportionately large uncompressed representation, which allows remote attackers to cause a denial of service (memory and CPU consumption, and application hang) via a crafted PNG file, as demonstrated by use of the deflate compression method on data composed of many occurrences of the same character, related to a decompression bomb attack.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204141
9542	CVE-2010-0097	Medium		ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta does not properly validate DNSSEC (1) NSEC and (2) NSEC3 records, which allows remote attackers to add the Authenticated Data (AD) flag to a forged NXDOMAIN response for an existing domain.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199176
9543	CVE-2010-0015	High		nis/nss_nis/nis-pwd.c in the GNU C Library (aka glibc or libc6) 2.7 and Embedded GLIBC (EGLIBC) 2.10.2 adds information from the passwd.adjunct.byname map to entries in the passwd map, which allows remote attackers to obtain the encrypted passwords of NIS accounts by calling the getpwnam function.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197001

	A	B	C	D	E	F	G	H	I	J	K	L	M
9544	CVE-2010-0010	Medium		Integer overflow in the ap_proxy_send_fb function in proxy/proxy_util.c in mod_proxy in the Apache HTTP Server before 1.3.42 on 64-bit platforms allows remote origin servers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a large chunk size that triggers a heap-based buffer overflow.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00200924
9545	CVE-2010-0008	High		The SCTP implementation in the Linux kernel before 2.6.23 allows remote attackers to cause a denial of service (infinite loop) via (1) an Out Of The Blue (OOTB) chunk or (2) a chunk of zero length.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202829
9546	CVE-2010-0007	Low		net/bridge/netfilter/ebtables.c in the ebtables module in the netfilter framework in the Linux kernel before 2.6.33-rc4 does not require the CAP_NET_ADMIN capability for setting or modifying rules, which allows local users to bypass intended access restrictions and configure arbitrary network-traffic filtering via a modified ebtables application.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199180
9547	CVE-2010-0006	High		The ipv6_hop_jumbo function in net/ipv6/exthdrs.c in the Linux kernel before 2.6.32.4, when network namespaces are enabled, allows remote attackers to cause a denial of service (NULL pointer dereference) via an invalid IPv6 jumbogram, a related issue to CVE-2007-4567.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199181
9548	CVE-2010-0003	Medium		The print_fatal_signal function in kernel/signal.c in the Linux kernel before 2.6.32.4 on the i386 platform, when printfatal-signals is enabled, allows local users to discover the contents of arbitrary memory locations by jumping to an address and then reading a log file, and might allow local users to cause a denial of service (system slowdown or crash) by jumping to an address.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00199179
9549	CVE-2010-0002	Low		The /etc/profile.d/60alias.sh script in the Mandriva bash package for Bash 2.05b, 3.0, 3.2, 3.2.48, and 4.0 enables the --show-control-chars option in LS_OPTIONS, which allows local users to send escape sequences to terminal emulators, or hide the existence of a file, via a crafted filename.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00196999
9550	CVE-2010-0001	Medium		Integer underflow in the unlzw function in unlzw.c in gzip before 1.4 on 64-bit platforms allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted archive that uses LZW compression, leading to an array index error.	gzip	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197985
9551	CVE-2009-5155	Medium	HIGH	In the GNU C Library (aka glibc or libc6) before 2.28, parse_reg_exp in posix/regcomp.c misparses alternatives, which allows attackers to cause a denial of service (assertion failure and application exit) or trigger an incorrect result by attempting a regular-expression match.	glibc	Unchanged	8.0.0.31	9.0.0.22	10.17.41.17	Not vulnerable	10.19.45.1	Not vulnerable	LIN1018-3699
9552	CVE-2009-5147	High		DL::dlopen in Ruby 1.8, 1.9.0, 1.9.2, 1.9.3, 2.0.0 before patchlevel 648, and 2.1 before 2.1.8 opens libraries with tainted names.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-3899
9553	CVE-2009-5146			A memory leak flaw was fix in the hostname TLS extension: https://github.com/openssl/openssl/commit/7587347bc48e7e8a1e800e48bb0a658f1557c424	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-465
9554	CVE-2009-5138	Medium		GnuTLS before 2.7.6, when the GNUTLS_VERIFY_ALLOW_X509_V1_CA_CRT flag is not enabled, treats version 1 X.509 certificates as intermediate CAs, which allows remote attackers to bypass intended restrictions by leveraging a X.509 V1 certificate from a trusted CA to issue new certificates, a different vulnerability than CVE-2014-1959.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN6-6958
9555	CVE-2009-5110	Medium		dhttpd allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00328004
9556	CVE-2009-5082	Low		The (1) configure and (2) config.guess scripts in GNU troff (aka groff) 1.20.1 on Openwall GNU/*/Linux (aka Owl) improperly create temporary files upon a failure of the mktemp function, which makes it easier for local users to overwrite arbitrary files via a symlink attack on a temporary file.	groff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286695
9557	CVE-2009-5081	Low		The (1) config.guess, (2) contrib/groffer/perl/groffer.pl, and (3) contrib/groffer/perl/roff2.pl scripts in GNU troff (aka groff) 1.21 and earlier use an insufficient number of X characters in the template argument to the tempfile function, which makes it easier for local users to overwrite arbitrary files via a symlink attack on a temporary file, a different vulnerability than CVE-2004-0969.	groff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286696
9558	CVE-2009-5080	Low		The (1) contrib/eqn2graph/eqn2graph.sh, (2) contrib/grap2graph/grap2graph.sh, and (3) contrib/pic2graph/pic2graph.sh scripts in GNU troff (aka groff) 1.21 and earlier do not properly handle certain failed attempts to create temporary directories, which might allow local users to overwrite arbitrary files via a symlink attack on a file in a temporary directory, a different vulnerability than CVE-2004-1296.	groff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286699
9559	CVE-2009-5079	Low		The (1) gendef.sh, (2) doc/fixinfo.sh, and (3) contrib/gdiffmk/tests/runtests.in scripts in GNU troff (aka groff) 1.21 and earlier allow local users to overwrite arbitrary files via a symlink attack on a gro#####.tmp or /tmp/##### temporary file.	groff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286698
9560	CVE-2009-5078	Medium		contrib/pdfmark/pdfroff.sh in GNU troff (aka groff) before 1.21 launches the Ghostscript program without the -dSAFER option, which allows remote attackers to create, overwrite, rename, or delete arbitrary files via a crafted document.	groff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286697

	A	B	C	D	E	F	G	H	I	J	K	L	M
9561	CVE-2009-5064	Medium		** DISPUTED ** ldd in the GNU C Library (aka glibc or libc6) 2.13 and earlier allows local users to gain privileges via a Trojan horse executable file linked with a modified loader that omits certain LD_TRACE_LOADED_OBJECTS checks. NOTE: the GNU C Library vendor states This is just nonsense. There are a gazillion other ways to introduce code if people are downloading arbitrary binaries and install them in appropriate directories or set LD_LIBRARY_PATH etc.	glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00266145
9562	CVE-2009-5063	Medium		Memory leak in pngwutil.c in libpng before 1.2.39beta5 allows context-dependent attackers to cause a denial of service (memory leak or segmentation fault) via a JPEG image containing an iCCP chunk with a negative embedded profile length. NOTE: this is due to an incomplete fix for CVE-2006-7244.	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299598
9563	CVE-2009-5044	Low		contrib/pdfmark/pdfroff.sh in GNU troff (aka groff) before 1.21 allows local users to overwrite arbitrary files via a symlink attack on a pdf######.tmp temporary file.	groff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00286700
9564	CVE-2009-5042			python-docutils allows insecure usage of temporary files	python-docutils	Unchanged	Investigate	Investigate	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN1018-5183
9565	CVE-2009-5029	Medium		Integer overflow in the __tzfile_read function in glibc before 2.15 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted timezone (TZ) file, as demonstrated using vsftpd.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00417557
9566	CVE-2009-5026	Medium		The executable comment feature in MySQL 5.0.x before 5.0.93 and 5.1.x before 5.1.50, when running in certain slave configurations in which the slave is running a newer version than the master, allows remote attackers to execute arbitrary SQL commands via custom comments.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00374003
9567	CVE-2009-5022	Medium		Heap-based buffer overflow in tif_ojpeg.c in the OJPEG decoder in LibTIFF before 3.9.5 allows remote attackers to execute arbitrary code via a crafted TIFF file.	libtiff.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00277728
9568	CVE-2009-4975	Medium		Cross-site scripting (XSS) vulnerability in webview.cpp in QtDemoBrowser allows remote attackers to inject arbitrary web script or HTML via a URL associated with a nonexistent domain name, related to a universal XSS issue, a similar vulnerability to CVE-2010-2536.	nokia qtdemobrowser.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00228511
9569	CVE-2009-4902	Medium		Buffer overflow in the MSGFunctionDemarshall function in winscard_svc.c in the PC/SC Smart Card daemon (aka PCSCD) in MUSCLE PCSC-Lite 1.5.4 and earlier might allow local users to gain privileges via crafted SCARD_CONTROL message data, which is improperly demarshalled. NOTE: this vulnerability exists because of an incorrect fix for CVE-2010-0407.	pcsc-lite.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00222223
9570	CVE-2009-4901	Low		The MSGFunctionDemarshall function in winscard_svc.c in the PC/SC Smart Card daemon (aka PCSCD) in MUSCLE PCSC-Lite before 1.5.4 might allow local users to cause a denial of service (daemon crash) via crafted SCARD_SET_ATTRIB message data, which is improperly demarshalled and triggers a buffer over-read, a related issue to CVE-2010-0407.	pcsc-lite.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00222229
9571	CVE-2009-4897	High		Buffer overflow in gs/psi/iscan.c in Ghostscript 8.64 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDF document containing a long name.	The PATCH for it is GPLv3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00223172
9572	CVE-2009-4895	Medium		Race condition in the tty_fasync function in drivers/char/tty_io.c in the Linux kernel before 2.6.32.6 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via unknown vectors, related to the put_tty_queue and __f_setown functions. NOTE: the vulnerability was addressed in a different way in 2.6.32.9.	Linux Kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218124
9573	CVE-2009-4881	Medium		Integer overflow in the __vstrfmon_l function in stdlib/strfmon_l.c in the strfmon implementation in the GNU C Library (aka glibc or libc6) before 2.10.1 allows context-dependent attackers to cause a denial of service (application crash) via a crafted format string, as demonstrated by the %9999999999999999999n string, a related issue to CVE-2008-1391.	gnu glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218804
9574	CVE-2009-4880	Medium		Multiple integer overflows in the strfmon implementation in the GNU C Library (aka glibc or libc6) 2.10.1 and earlier allow context-dependent attackers to cause a denial of service (memory consumption or application crash) via a crafted format string, as demonstrated by a crafted first argument to the money_format function in PHP, a related issue to CVE-2008-1391.	gnu glibc.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218803
9575	CVE-2009-4835	Medium		The (1) htk_read_header, (2) alaw_init, (3) ulaw_init, (4) pcm_init, (5) float32_init, and (6) sds_read_header functions in libsndfile 1.0.20 allow context-dependent attackers to cause a denial of service ((divide-by-zero error and application crash) via a crafted audio file.	libsndfile	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00213410
9576	CVE-2009-4833	Medium		MySQL Connector/NET before 6.0.4, when using encryption, does not verify SSL certificates during connection, which allows remote attackers to perform a man-in-the-middle attack with a spoofed SSL certificate.	MySQL Connector/ NET	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00211190
9577	CVE-2009-4810	High		The Secure Remote Password (SRP) implementation in Samhain before 2.5.4 does not check for a certain zero value where required by the protocol, which allows remote attackers to bypass authentication via crafted input.	samhain	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00211191

	A	B	C	D	E	F	G	H	I	J	K	L	M
9578	CVE-2009-4565	High		sendmail before 8.14.4 does not properly handle a '\0' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	sendmail	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197009
9579	CVE-2009-4538	High		drivers/net/e1000e/netdev.c in the e1000e driver in the Linux kernel 2.6.32.3 and earlier does not properly check the size of an Ethernet frame that exceeds the MTU, which allows remote attackers to have an unspecified impact via crafted packets, a related issue to CVE-2009-4537.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197002
9580	CVE-2009-4537	High		drivers/net/r8169.c in the r8169 driver in the Linux kernel 2.6.32.3 and earlier does not properly check the size of an Ethernet frame that exceeds the MTU, which allows remote attackers to (1) cause a denial of service (temporary network outage) via a packet with a crafted size, in conjunction with certain packets containing A characters and certain packets containing E characters; or (2) cause a denial of service (system crash) via a packet with a crafted size, in conjunction with certain packets containing \0' characters, related to the value of the status register and erroneous behavior associated with the RxMaxSize register. NOTE: this vulnerability exists because of an incorrect fix for CVE-2009-1389.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197005
9581	CVE-2009-4536	High		drivers/net/e1000/e1000_main.c in the e1000 driver in the Linux kernel 2.6.32.3 and earlier handles Ethernet frames that exceed the MTU by processing certain trailing payload data as if it were a complete frame, which allows remote attackers to bypass packet filters via a large packet with a crafted payload. NOTE: this vulnerability exists because of an incorrect fix for CVE-2009-1385.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197003
9582	CVE-2009-4496	Medium		Boa 0.94.14rc21 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	boa	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197000
9583	CVE-2009-4492	Medium		WEBrick 1.3.1 in Ruby 1.8.6 through patchlevel 383, 1.8.7 through patchlevel 248, 1.8.8dev, 1.9.1 through patchlevel 376, and 1.9.2dev writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197006
9584	CVE-2009-4484	High		Buffer overflow in the server in MySQL 5.0.51a on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by the vd_mysql5 module in VulnDisco Pack Professional 8.11. NOTE: as of 20091229, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00195724
9585	CVE-2009-4481	Medium		Unspecified vulnerability in radiusd in FreeRADIUS 1.1.7 allows remote attackers to cause a denial of service (daemon crash) via unknown vectors, as demonstrated by a certain module in VulnDisco Pack Professional 7.6 through 8.11. NOTE: as of 20091229, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	FreeRADIUS	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00195730
9586	CVE-2009-4457	High		Multiple unspecified vulnerabilities in the Vsftpd Webmin module before 1.3b for the Vsftpd server have unknown impact and attack vectors related to Some security issues.	Vsftpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00195728
9587	CVE-2009-4411	Low		The (1) setfacl and (2) getfacl commands in XFS acl 2.2.47, when running in recursive (-R) mode, follow symbolic links even when the --physical (aka -P) or -L option is specified, which might allow local users to modify the ACL for arbitrary files or directories via a symlink attack.	XFS	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00195726
9588	CVE-2009-4410	Medium		The fuse_ioctl_copy_user function in the ioctl handler in fs/fuse/file.c in the Linux kernel 2.6.29-rc1 through 2.6.30.y uses the wrong variable in an argument to the kunmap function, which allows local users to cause a denial of service (panic) via unknown vectors.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00195731
9589	CVE-2009-4355	Medium		Memory leak in the zlib_stateful_finish function in crypto/comp/c_zlib.c in OpenSSL 0.9.8l and earlier and 1.0.0 Beta through Beta 4 allows remote attackers to cause a denial of service (memory consumption) via vectors that trigger incorrect calls to the CRYPTO_free_all_ex_data function, as demonstrated by use of SSLv3 and PHP with the Apache HTTP Server, a related issue to CVE-2008-1678.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197007
9590	CVE-2009-4308	High		The ext4_decode_error function in fs/ext4/super.c in the ext4 filesystem in the Linux kernel before 2.6.32 allows user-assisted remote attackers to cause a denial of service (NULL pointer dereference), and possibly have unspecified other impact, via a crafted read-only filesystem that lacks a journal.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194861
9591	CVE-2009-4307	High		The ext4_fill_flex_info function in fs/ext4/super.c in the Linux kernel before 2.6.32-git6 allows user-assisted remote attackers to cause a denial of service (divide-by-zero error and panic) via a malformed ext4 filesystem containing a super block with a large FLEX_BG group size (aka s_log_groups_per_flex value).	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194771

	A	B	C	D	E	F	G	H	I	J	K	L	M
9592	CVE-2009-4306	Medium		Unspecified vulnerability in the EXT4_IOC_MOVE_EXT (aka move extents) ioctl implementation in the ext4 filesystem in the Linux kernel 2.6.32-git6 and earlier allows local users to cause a denial of service (filesystem corruption) via unknown vectors, a different vulnerability than CVE-2009-4131.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194768
9593	CVE-2009-4272	High		A certain Red Hat patch for net/ipv4/route.c in the Linux kernel 2.6.18 on Red Hat Enterprise Linux (RHEL) 5 allows remote attackers to cause a denial of service (deadlock) via crafted packets that force collisions in the IPv4 routing hash table, and trigger a routing emergency in which a hash chain is too long. NOTE: this is related to an issue in the Linux kernel before 2.6.31, when the kernel routing cache is disabled, involving an uninitialized pointer and a panic.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197961
9594	CVE-2009-4271	Medium		The Linux kernel 2.6.9 through 2.6.17 on the x86_64 and amd64 platforms allows local users to cause a denial of service (panic) via a 32-bit application that calls mprotect on its Virtual Dynamic Shared Object (VDSO) page and then triggers a segmentation fault.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204097
9595	CVE-2009-4235	Medium		acpid 1.0.4 sets an unrestrictive umask, which might allow local users to leverage weak permissions on /var/log/acpid, and obtain sensitive information by reading this file or cause a denial of service by overwriting this file, a different vulnerability than CVE-2009-4033.	acpid	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194767
9596	CVE-2009-4212	High		Multiple integer underflows in the (1) AES and (2) RC4 decryption functionality in the crypto library in MIT Kerberos 5 (aka krb5) 1.3 through 1.6.3, and 1.7 before 1.7.1, allow remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code by providing ciphertext with a length that is too short to be valid.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197004
9597	CVE-2009-4141	High		Use-after-free vulnerability in the fasync_helper function in fs/fcntl.c in the Linux kernel before 2.6.33-rc4-git1 allows local users to gain privileges via vectors that include enabling O_ASYNC (aka FASYNC or FIOASYNC) on a locked file, and then closing this file.Per: http://cwe.mitre.org/data/definitions/416.html CWE-416: Use After Free	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197593
9598	CVE-2009-4138	Medium		drivers/firewire/ohci.c in the Linux kernel before 2.6.32-git9, when packet-per-buffer mode is used, allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unknown other impact via an unspecified ioctl associated with receiving an ISO packet that contains zero in the payload-length field.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00195729
9599	CVE-2009-4136	Medium		PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly manage session-local state during execution of an index function by a database superuser, which allows remote authenticated users to gain privileges via a table with crafted index functions, as demonstrated by functions that modify (1) search_path or (2) a prepared statement, a related issue to CVE-2007-6600 and CVE-2009-3230.	postgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194855
9600	CVE-2009-4135	Medium		The distcheck rule in dist-check.mk in GNU coreutils 5.2.1 through 8.1 allows local users to gain privileges via a symlink attack on a file in a directory tree under /tmp.	The PATCH for it is GPLv3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194857
9601	CVE-2009-4134	Medium		Buffer underflow in the rgbimg module in Python 2.5 allows remote attackers to cause a denial of service (application crash) via a large ZSIZE value in a black-and-white (aka B/W) RGB image that triggers an invalid pointer dereference.	Python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00211612
9602	CVE-2009-4131	High		The EXT4_IOC_MOVE_EXT (aka move extents) ioctl implementation in the ext4 filesystem in the Linux kernel before 2.6.32-git6 allows local users to overwrite arbitrary files via a crafted request, related to insufficient checks for file permissions.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194766
9603	CVE-2009-4128	High		GNU GRand Unified Bootloader (GRUB) 2 1.97 only compares the submitted portion of a password with the actual password, which makes it easier for physically proximate attackers to conduct brute force attacks and bypass authentication by submitting a password whose length is 1.	GRUB	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194860
9604	CVE-2009-4124	High		Heap-based buffer overflow in the rb_str_justify function in string.c in Ruby 1.9.1 before 1.9.1-p376 allows context-dependent attackers to execute arbitrary code via unspecified vectors involving (1) String#ljust, (2) String#center, or (3) String#rjust. NOTE: some of these details are obtained from third party information.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194856
9605	CVE-2009-4034	Medium		PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based PostgreSQL servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended client-hostname restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	postgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194774
9606	CVE-2009-4033	Medium		A certain Red Hat patch for acpid 1.0.4 effectively triggers a call to the open function with insufficient arguments, which might allow local users to leverage weak permissions on /var/log/acpid, and obtain sensitive information by reading this file, cause a denial of service by overwriting this file, or gain privileges by executing this file.	acpid	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194769

	A	B	C	D	E	F	G	H	I	J	K	L	M
9607	CVE-2009-4031	High		The do_insn_fetch function in arch/x86/kvm/emulate.c in the x86 emulator in the KVM subsystem in the Linux kernel before 2.6.32-rc8-next-20091125 tries to interpret instructions that contain too many bytes to be valid, which allows guest OS users to cause a denial of service (increased scheduling latency) on the host OS via unspecified manipulations related to SMP support.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193855
9608	CVE-2009-4030	Medium		MySQL 5.1.x before 5.1.41 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL data home directory, related to incorrect calculation of the mysql_unpacked_real_data_home value. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4098 and CVE-2008-2079.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193784
9609	CVE-2009-4029	Medium		The (1) dist or (2) distcheck rules in GNU Automake 1.11.1, 1.10.3, and release branches branch-1-4 through branch-1-9, when producing a distribution tarball for a package that uses Automake, assign insecure permissions (777) to directories in the build tree, which introduces a race condition that allows local users to modify the contents of package files, introduce Trojan horse programs, or conduct other attacks before the build is complete.	Automake	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00195727
9610	CVE-2009-4028	Medium		The vio_verify_callback function in viossl\factories.c in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41, when OpenSSL is used, accepts a value of zero for the depth of X.509 certificates, which allows man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certificate, as demonstrated by a certificate presented by a server linked against the yaSSL library.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193781
9611	CVE-2009-4027	High		Race condition in the mac80211 subsystem in the Linux kernel before 2.6.32-rc8-next-20091201 allows remote attackers to cause a denial of service (system crash) via a Delete Block ACK (aka DELBA) packet that triggers a certain state change in the absence of an aggregation session.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194765
9612	CVE-2009-4026	High		The mac80211 subsystem in the Linux kernel before 2.6.32-rc8-next-20091201 allows remote attackers to cause a denial of service (panic) via a crafted Delete Block ACK (aka DELBA) packet, related to an erroneous code shuffling patch.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194859
9613	CVE-2009-4022	Medium		Unspecified vulnerability in ISC BIND 9.4 before 9.4.3-P4, 9.5 before 9.5.2-P1, 9.6 before 9.6.1-P2, 9.7 beta before 9.7.0b3, and 9.0.x through 9.3.x with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks via additional sections in a response sent for resolution of a recursive client query, which is not properly handled when the response is processed at the same time as requesting DNSSEC records (DO).	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193857
9614	CVE-2009-4021	Medium		The fuse_direct_io function in fs/fuse/file.c in the fuse subsystem in the Linux kernel before 2.6.32-rc7 might allow attackers to cause a denial of service (invalid pointer dereference and OOPS) via vectors possibly related to a memory-consumption attack.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193853
9615	CVE-2009-4020	High		Stack-based buffer overflow in the hfs subsystem in the Linux kernel 2.6.32 allows remote attackers to have an unspecified impact via a crafted Hierarchical File System (HFS) filesystem, related to the hfs_readdir function in fs/hfs/dir.c.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194858
9616	CVE-2009-4019	Medium		mysqld in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 does not (1) properly handle errors during execution of certain SELECT statements with subqueries, and does not (2) preserve certain null_value flags during execution of statements that use the GeomFromWKB function, which allows remote authenticated users to cause a denial of service (daemon crash) via a crafted statement.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193782
9617	CVE-2009-4005	High		The collect_rx_frame function in drivers/isdn/hisax/hfc_usb.c in the Linux kernel before 2.6.32-rc7 allows attackers to have an unspecified impact via a crafted HDLC packet that arrives over ISDN and triggers a buffer under-read.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193776
9618	CVE-2009-4004	High		Buffer overflow in the kvm_vcpu_ioctl_x86_setup_mce function in arch/x86/kvm/x86.c in the KVM subsystem in the Linux kernel before 2.6.32-rc7 allows local users to cause a denial of service (memory corruption) or possibly gain privileges via a KVM_X86_SETUP_MCE IOCTL request that specifies a large number of Machine Check Exception (MCE) banks.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193854
9619	CVE-2009-3939	Medium		The poll_mode_io file for the megaraid_sas driver in the Linux kernel 2.6.31.6 and earlier has world-writable permissions, which allows local users to change the I/O mode of the driver by modifying this file.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193777
9620	CVE-2009-3889	Medium		The dbg_lvl file for the megaraid_sas driver in the Linux kernel before 2.6.27 has world-writable permissions, which allows local users to change the (1) behavior and (2) logging level of the driver by modifying this file.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193780
9621	CVE-2009-3888	Medium		The do_mmap_pgoff function in mm/nommu.c in the Linux kernel before 2.6.31.6, when the CPU lacks a memory management unit, allows local users to cause a denial of service (OOPS) via an application that attempts to allocate a large amount of memory.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193856

	A	B	C	D	E	F	G	H	I	J	K	L	M
9622	CVE-2009-3767	Medium		libraries/libldap/tls_o.c in OpenLDAP, when OpenSSL is used, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189611
9623	CVE-2009-3743	High		Off-by-one error in the TrueType bytecode interpreter in Ghostscript before 8.71 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a malformed TrueType font in a document.	ghostscript	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00232302
9624	CVE-2009-3736	Medium		ltdl.c in libltdl in GNU Libtool 1.5.x, and 2.2.6 before 2.2.6b, attempts to open a .la file in the current working directory, which allows local users to gain privileges via a Trojan horse file.	Libtool	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193783
9625	CVE-2009-3726	High		The nfs4_proc_lock function in fs/nfs/nfs4proc.c in the NFSv4 client in the Linux kernel before 2.6.31-rc4 allows remote NFS servers to cause a denial of service (NULL pointer dereference and panic) by sending a certain response containing incorrect file attributes, which trigger attempted use of an open file that lacks NFSv4 state.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00191376
9626	CVE-2009-3725	High		The connector layer in the Linux kernel before 2.6.31.5 does not require the CAP_SYS_ADMIN capability for certain interaction with the (1) uvesafb, (2) pohmelfs, (3) dst, or (4) dm subsystem, which allows local users to bypass intended access restrictions and gain privileges via calls to functions in these subsystems.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00191378
9627	CVE-2009-3722	High		The handle_dr function in arch/x86/kvm/vmx.c in the KVM subsystem in the Linux kernel before 2.6.31.1 does not properly verify the Current Privilege Level (CPL) before accessing a debug register, which allows guest OS users to cause a denial of service (trap) on the host OS via a crafted application.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189684
9628	CVE-2009-3720	Medium		The updatePosition function in lib/xmltok_impl.c in libexpat in Expat 2.0.1, as used in Python, PyXML, w3c-libwww, and other software, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with crafted UTF-8 sequences that trigger a buffer over-read, a different vulnerability than CVE-2009-2625.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00191375
9629	CVE-2009-3640	Low		The update_cr8_intercept function in arch/x86/kvm/x86.c in the KVM subsystem in the Linux kernel before 2.6.32-rc1 does not properly handle the absence of an Advanced Programmable Interrupt Controller (APIC), which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly gain privileges via a call to the kvm_vcpu_ioctl function.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189614
9630	CVE-2009-3638	High		Integer overflow in the kvm_dev_ioctl_get_supported_cpuid function in arch/x86/kvm/x86.c in the KVM subsystem in the Linux kernel before 2.6.31.4 allows local users to have an unspecified impact via a KVM_GET_SUPPORTED_CPUID request to the kvm_arch_dev_ioctl function.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189680
9631	CVE-2009-3626	Medium		Perl 5.10.1 allows context-dependent attackers to cause a denial of service (application crash) via a UTF-8 character with a large, invalid codepoint, which is not properly handled during a regular-expression match.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189613
9632	CVE-2009-3624	Medium		The get_instantiation_keyring function in security/keys/keyctl.c in the KEYS subsystem in the Linux kernel before 2.6.32-rc5 does not properly maintain the reference count of a keyring, which allows local users to gain privileges or cause a denial of service (OOPS) via vectors involving calls to this function without specifying a keyring by ID, as demonstrated by a series of keyctl request2 and keyctl list commands.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00191374
9633	CVE-2009-3623	High		The lookup_cb_cred function in fs/nfsd/nfs4callback.c in the nfsd4 subsystem in the Linux kernel before 2.6.31.2 attempts to access a credentials cache even when a client specifies the AUTH_NULL authentication flavor, which allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via an NFSv4 mount request.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189682
9634	CVE-2009-3621	Medium		net/unix/af_unix.c in the Linux kernel 2.6.31.4 and earlier allows local users to cause a denial of service (system hang) by creating an abstract-namespace AF_UNIX listening socket, performing a shutdown operation on this socket, and then performing a series of connect operations to this socket.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189681
9635	CVE-2009-3620	Medium		The ATI Rage 128 (aka r128) driver in the Linux kernel before 2.6.31-git11 does not properly verify Concurrent Command Engine (CCE) state initialization, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly gain privileges via unspecified ioctl calls.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189677
9636	CVE-2009-3616	High		Multiple use-after-free vulnerabilities in vnc.c in the VNC server in QEMU 0.10.6 and earlier might allow guest OS users to execute arbitrary code on the host OS by establishing a connection from a VNC client and then (1) disconnecting during data transfer, (2) sending a message using incorrect integer data types, or (3) using the Fuzzy Screen Mode protocol, related to double free vulnerabilities.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189683
9637	CVE-2009-3613	High		The swiotlb functionality in the r8169 driver in drivers/net/r8169.c in the Linux kernel before 2.6.27.22 allows remote attackers to cause a denial of service (IOMMU space exhaustion and system crash) by using jumbo frames for a large amount of network traffic, as demonstrated by a flood ping.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189612

	A	B	C	D	E	F	G	H	I	J	K	L	M
9638	CVE-2009-3612	Medium		The tcf_fill_node function in net/sched/cls_api.c in the netlink subsystem in the Linux kernel 2.6.x before 2.6.32-rc5, and 2.4.37.6 and earlier, does not initialize a certain tcm__pad2 structure member, which might allow local users to obtain sensitive information from kernel memory via unspecified vectors. NOTE: this issue exists because of an incomplete fix for CVE-2005-4881.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189610
9639	CVE-2009-3563	Medium		ntp_request.c in ntpd in NTP before 4.2.4p8, and 4.2.5, allows remote attackers to cause a denial of service (CPU and bandwidth consumption) by using MODE_PRIVATE to send a spoofed (1) request or (2) response packet that triggers a continuous exchange of MODE_PRIVATE error responses between two NTP daemons.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194773
9640	CVE-2009-3560	Medium		The big2_toUtf8 function in lib/xmltok.c in libexpat in Expat 2.0.1, as used in the XML-Twig module for Perl, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with malformed UTF-8 sequences that trigger a buffer over-read, related to the doProlog function in lib/xmlparse.c, a different vulnerability than CVE-2009-2625 and CVE-2009-3720.	Expat	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194772
9641	CVE-2009-3556	Low		A certain Red Hat configuration step for the qla2xxx driver in the Linux kernel 2.6.18 on Red Hat Enterprise Linux (RHEL) 5, when N_Port ID Virtualization (NPIV) hardware is used, sets world-writable permissions for the (1) vport_create and (2) vport_delete files under /sys/class/scsi_host/, which allows local users to make arbitrary changes to SCSI host attributes by modifying these files.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197964
9642	CVE-2009-3555	Medium		The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a plaintext injection attack, aka the Project Mogul issue.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00190505
9643	CVE-2009-3547	Medium		Multiple race conditions in fs/pipe.c in the Linux kernel before 2.6.32-rc6 allow local users to cause a denial of service (NULL pointer dereference and system crash) or gain privileges by attempting to open an anonymous pipe via a /proc/*/fd/ pathname.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00191377
9644	CVE-2009-3490	Medium		GNU Wget before 1.12 does not properly handle a \0' character in a domain name in the Common Name field of an X.509 certificate, which allows man-in-the-middle remote attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	The PATCH for it is GPLv3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185837
9645	CVE-2009-3297	REJECT		** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2010-0787, CVE-2010-0788, CVE-2010-0789. Reason: this candidate was intended for one issue in Samba, but it was used for multiple distinct issues, including one in FUSE and one in ncpfs. Notes: All CVE users should consult CVE-2010-0787 (Samba), CVE-2010-0788 (ncpfs), and CVE-2010-0789 (FUSE) to determine which ID is appropriate. All references and descriptions in this candidate have been removed to prevent accidental usage.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00198003
9646	CVE-2009-3295	High		The prep_reprocess_req function in kdc/do_tgs_req.c in the cross-realm referral implementation in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.7 before 1.7.1 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a ticket request.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00195725
9647	CVE-2009-3290	High		The kvm_emulate_hypercall function in arch/x86/kvm/x86.c in KVM in the Linux kernel 2.6.25-rc1, and other versions before 2.6.31, when running on x86 systems, does not prevent access to MMU hypercalls from ring 0, which allows local guest OS users to cause a denial of service (guest kernel crash) and read or write guest kernel memory via unspecified random addresses.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185843
9648	CVE-2009-3289	Medium		The g_file_copy function in glib 2.0 sets the permissions of a target file to the permissions of a symbolic link (777), which allows user-assisted local users to modify files of other users, as demonstrated by using Nautilus to modify the permissions of the user home directory.	glib	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185833
9649	CVE-2009-3288	Medium		The sg_build_indirect function in drivers/scsi/sg.c in Linux kernel 2.6.28-rc1 through 2.6.31-rc8 uses an incorrect variable when accessing an array, which allows local users to cause a denial of service (kernel OOPS and NULL pointer dereference), as demonstrated by using xcdroast to duplicate a CD. NOTE: this is only exploitable by users who can open the cdrom device.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185842
9650	CVE-2009-3286	Medium		NFSv4 in the Linux kernel 2.6.18, and possibly other versions, does not properly clean up an inode when an O_EXCL create fails, which causes files to be created with insecure settings such as setuid bits, and possibly allows local users to gain privileges, related to the execution of the do_open_permission function even when a create fails.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185853

	A	B	C	D	E	F	G	H	I	J	K	L	M
9651	CVE-2009-3280	High		Integer signedness error in the find_ie function in net/wireless/scan.c in the cfg80211 subsystem in the Linux kernel before 2.6.31.1-rc1 allows remote attackers to cause a denial of service (soft lockup) via malformed packets.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185841
9652	CVE-2009-3245	High		OpenSSL before 0.9.8m does not check for a NULL return value from bn_wexpand function calls in (1) crypto/bn/bn_div.c, (2) crypto/bn/bn_gf2m.c, (3) crypto/ec/ec2_smpl.c, and (4) engines/e_ubsec.c, which has unspecified impact and context-dependent attack vectors.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00204144
9653	CVE-2009-3238	High		The get_random_int function in drivers/char/random.c in the Linux kernel before 2.6.30 produces insufficiently random numbers, which allows attackers to predict the return value, and possibly defeat protection mechanisms based on randomization, via vectors that leverage the function's tendency to return the same value over and over again for long stretches of time.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185835
9654	CVE-2009-3234	Medium		Buffer overflow in the perf_copy_attr function in kernel/perf_counter.c in the Linux kernel 2.6.31-rc1 allows local users to cause a denial of service (crash) and execute arbitrary code via a big size data to the perf_counter_open system call.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185836
9655	CVE-2009-3232	High		pam-auth-update for PAM, as used in Ubuntu 8.10 and 9.4, and Debian GNU/Linux, does not properly handle an empty selection for system authentication modules in certain rare configurations, which causes any attempt to be successful and allows remote attackers to bypass authentication.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185832
9656	CVE-2009-3231	Medium		The core server component in PostgreSQL 8.3 before 8.3.8 and 8.2 before 8.2.14, when using LDAP authentication with anonymous binds, allows remote attackers to bypass authentication via an empty password.	postgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185840
9657	CVE-2009-3230	Medium		The core server component in PostgreSQL 8.4 before 8.4.1, 8.3 before 8.3.8, 8.2 before 8.2.14, 8.1 before 8.1.18, 8.0 before 8.0.22, and 7.4 before 7.4.26 does not use the appropriate privileges for the (1) RESET ROLE and (2) RESET SESSION AUTHORIZATION operations, which allows remote authenticated users to gain privileges. NOTE: this is due to an incomplete fix for CVE-2007-6600.	postgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185839
9658	CVE-2009-3229	Medium		The core server component in PostgreSQL 8.4 before 8.4.1, 8.3 before 8.3.8, and 8.2 before 8.2.14 allows remote authenticated users to cause a denial of service (backend shutdown) by re-LOAD-ing libraries from a certain plugins directory.	postgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185844
9659	CVE-2009-3228	Medium		The tc_fill_tclass function in net/sched/sch_api.c in the tc subsystem in the Linux kernel 2.4.x before 2.4.37.6 and 2.6.x before 2.6.31-rc9 does not initialize certain (1) tcm__pad1 and (2) tcm__pad2 structure members, which might allow local users to obtain sensitive information from kernel memory via unspecified vectors.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189609
9660	CVE-2009-3111	Medium		The rad_decode function in FreeRADIUS before 1.1.8 allows remote attackers to cause a denial of service (radiusd crash) via zero-length Tunnel-Password attributes. NOTE: this is a regression error related to CVE-2003-0967.	FreeRADIUS	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00182765
9661	CVE-2009-3095	High		The mod_proxy_ftp module in the Apache HTTP Server allows remote attackers to bypass intended access restrictions and send arbitrary commands to an FTP server via vectors related to the embedding of these commands in the Authorization HTTP header, as demonstrated by a certain module in VulnDisco Pack Professional 8.11. NOTE: as of 20090903, this disclosure has no actionable information. However, because the VulnDisco Pack author is a reliable researcher, the issue is being assigned a CVE identifier for tracking purposes.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00182767
9662	CVE-2009-3094	Medium		The ap_proxy_ftp_handler function in modules/proxy/proxy_ftp.c in the mod_proxy_ftp module in the Apache HTTP Server 2.0.63 and 2.2.13 allows remote FTP servers to cause a denial of service (NULL pointer dereference and child process crash) via a malformed reply to an EPSV command.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00182764
9663	CVE-2009-3080	High		Array index error in the gdth_read_event function in drivers/scsi/gdth.c in the Linux kernel before 2.6.32-rc8 allows local users to cause a denial of service or possibly gain privileges via a negative event index in an IOCTL request.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193778
9664	CVE-2009-3043	Medium		The tty_ldisc_hangup function in drivers/char/tty_ldisc.c in the Linux kernel before 2.6.31-rc8 allows local users to cause a denial of service (system crash, sometimes preceded by a NULL pointer dereference) or possibly gain privileges via certain pseudo-terminal I/O activity, as demonstrated by KernelTtyTest.c.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00182768
9665	CVE-2009-3002	Medium		The Linux kernel before 2.6.31-rc7 does not initialize certain data structures within getname functions, which allows local users to read the contents of some kernel memory locations by calling getsockname on (1) an AF_APPLETALK socket, related to the atalk_getname function in net/appletalk/ddp.c; (2) an AF_IRDA socket, related to the irda_getname function in net/irda/af_irda.c; (3) an AF_ECONET socket, related to the econet_getname function in net/econet/af_econet.c; (4) an AF_NETROM socket, related to the nr_getname function in net/netrom/af_netrom.c; (5) an AF_ROSE socket, related to the rose_getname function in net/rose/af_rose.c; or (6) a raw CAN socket, related to the raw_getname function in net/can/raw.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180266

	A	B	C	D	E	F	G	H	I	J	K	L	M
9666	CVE-2009-3001	Medium		The llc_ui_getname function in net/llc/af_llc.c in the Linux kernel 2.6.31-rc7 and earlier does not initialize a certain data structure, which allows local users to read the contents of some kernel memory locations by calling getsockname on an AF_LLC socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180265
9667	CVE-2009-2948	Low		mount.cifs in Samba 3.0 before 3.0.37, 3.2 before 3.2.15, 3.3 before 3.3.8 and 3.4 before 3.4.2, when mount.cifs is installed suid root, does not properly enforce permissions, which allows local users to read part of the credentials file and obtain the password by specifying the path to the credentials file and using the --verbose or -v option.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00187713
9668	CVE-2009-2910	Medium		arch/x86/ia32/ia32entry.S in the Linux kernel before 2.6.31.4 on the x86_64 platform does not clear certain kernel registers before a return to user mode, which allows local users to read register values from an earlier process by switching an ia32 process to 64-bit mode.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189616
9669	CVE-2009-2909	Medium		Integer signedness error in the ax25_setsockopt function in net/ax25/af_ax25.c in the ax25 subsystem in the Linux kernel before 2.6.31.2 allows local users to cause a denial of service (OOPS) via a crafted optlen value in an SO_BINDTODEVICE operation.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189615
9670	CVE-2009-2908	Medium		The d_delete function in fs/ecryptfs/inode.c in eCryptfs in the Linux kernel 2.6.31 allows local users to cause a denial of service (kernel OOPS) and possibly execute arbitrary code via unspecified vectors that cause a negative dentry and trigger a NULL pointer dereference, as demonstrated via a Mutt temporary directory in an eCryptfs mount.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00187710
9671	CVE-2009-2906	Medium		smbd in Samba 3.0 before 3.0.37, 3.2 before 3.2.15, 3.3 before 3.3.8, and 3.4 before 3.4.2 allows remote authenticated users to cause a denial of service (infinite loop) via an unanticipated oplock break notification reply packet.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00187711
9672	CVE-2009-2905	Medium		Heap-based buffer overflow in textbox.c in newt 0.51.5, 0.51.6, and 0.52.2 allows local users to cause a denial of service (application crash) or possibly execute arbitrary code via a request to display a crafted text dialog box.	newt	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185838
9673	CVE-2009-2904	Medium		A certain Red Hat modification to the ChrootDirectory feature in OpenSSH 4.8, as used in sshd in OpenSSH 4.3 in Red Hat Enterprise Linux (RHEL) 5.4 and Fedora 11, allows local users to gain privileges via hard links to setuid programs that use configuration files within the chroot directory, related to requirements for directory ownership.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00187709
9674	CVE-2009-2903	High		Memory leak in the appletalk subsystem in the Linux kernel 2.4.x through 2.4.37.6 and 2.6.x through 2.6.31, when the appletalk and ipddp modules are loaded but the ipddpN device is not found, allows remote attackers to cause a denial of service (memory consumption) via IP-DDP datagrams.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00182766
9675	CVE-2009-2849	Medium		The md driver (drivers/md/md.c) in the Linux kernel before 2.6.30.2 might allow local users to cause a denial of service (NULL pointer dereference) via vectors related to suspend_* sysfs attributes and the (1) suspend_lo_store or (2) suspend_hi_store functions. NOTE: this is only a vulnerability when sysfs is writable by an attacker.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180264
9676	CVE-2009-2848	Medium		The execve function in the Linux kernel, possibly 2.6.30-rc6 and earlier, does not properly clear the current->clear_child_tid pointer, which allows local users to cause a denial of service (memory corruption) via a clone system call with CLONE_CHILD_SETTID or CLONE_CHILD_CLEARTID enabled, which is not properly handled during thread creation and exit.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180262
9677	CVE-2009-2847	Medium		The do_sigaltstack function in kernel/signal.c in Linux kernel 2.4 through 2.4.37 and 2.6 before 2.6.31-rc5, when running on 64-bit systems, does not clear certain padding bytes from a structure, which allows local users to obtain sensitive information from the kernel stack via the sigaltstack function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180268
9678	CVE-2009-2846	High		The eisa_eeprom_read function in the parisc isa-eeprom component (drivers/parisc/eisa_eeprom.c) in the Linux kernel before 2.6.31-rc6 allows local users to access restricted memory via a negative ppos argument, which bypasses a check that assumes that ppos is positive and causes an out-of-bounds read in the readb function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180259
9679	CVE-2009-2844	High		cfg80211 in net/wireless/scan.c in the Linux kernel 2.6.30-rc1 and other versions before 2.6.31-rc6 allows remote attackers to cause a denial of service (crash) via a sequence of beacon frames in which one frame omits an SSID Information Element (IE) and the subsequent frame contains an SSID IE, which triggers a NULL pointer dereference in the cmp_ies function. NOTE: a potential weakness in the is_mesh function was also addressed, but the relevant condition did not exist in the code, so it is not a vulnerability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180269
9680	CVE-2009-2768	Medium		The load_flat_shared_library function in fs/binfmt_flat.c in the flat subsystem in the Linux kernel before 2.6.31-rc6 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by executing a shared flat binary.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177755
9681	CVE-2009-2767	High		The init_posix_timers function in kernel/posix-timers.c in the Linux kernel before 2.6.31-rc6 allows local users to cause a denial of service (OOPS) or possibly gain privileges via a CLOCK_MONOTONIC_RAW clock_nanosleep call that triggers a NULL pointer dereference.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177756

	A	B	C	D	E	F	G	H	I	J	K	L	M
9682	CVE-2009-2730	High		libgnutls in GnuTLS before 2.8.2 does not properly handle a '\0' character in a domain name in the subject's (1) Common Name (CN) or (2) Subject Alternative Name (SAN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.	GnuTLS	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177762
9683	CVE-2009-2711	Medium		XScreenSaver in Sun Solaris 9 and 10, OpenSolaris before snv_120, and X11 6.4.1 for Solaris 8, when the Xorg or Xnewt server is used, allows physically proximate attackers to obtain sensitive information by reading popup windows, which are displayed even when the screen is locked, a different vulnerability than CVE-2009-1276.	Xorg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177761
9684	CVE-2009-2699	Medium		The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00187712
9685	CVE-2009-2698	High		The udp_sendmsg function in the UDP implementation in (1) net/ipv4/udp.c and (2) net/ipv6/udp.c in the Linux kernel before 2.6.19 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via vectors involving the MSG_MORE flag and a UDP socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180260
9686	CVE-2009-2695	High		The Linux kernel before 2.6.31-rc7 does not properly prevent mmap operations that target page zero and other low memory addresses, which allows local users to gain privileges by exploiting NULL pointer dereference vulnerabilities, related to (1) the default configuration of the allow_unconfined_mmap_low boolean in SELinux on Red Hat Enterprise Linux (RHEL) 5, (2) an error that causes allow_unconfined_mmap_low to be ignored in the unconfined_t domain, (3) lack of a requirement for the CAP_SYS_RAWIO capability for these mmap operations, and (4) interaction between the mmap_min_addr protection mechanism and certain application programs.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180270
9687	CVE-2009-2692	High		The Linux kernel 2.6.0 through 2.6.30.4, and 2.4.4 through 2.4.37.4, does not initialize all function pointers for socket operations in proto_ops structures, which allows local users to trigger a NULL pointer dereference and gain privileges by using mmap to map page zero, placing arbitrary code on this page, and then invoking an unavailable operation, as demonstrated by the sendpage operation (sock_sendpage function) on a PF_PPPOX socket.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177764
9688	CVE-2009-2691	Low		The mm_for_maps function in fs/proc/base.c in the Linux kernel 2.6.30.4 and earlier allows local users to read (1) maps and (2) smaps files under proc/ via vectors related to ELF loading, a setuid process, and a race condition.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177754
9689	CVE-2009-2632	Medium		Buffer overflow in the SIEVE script component (sieve/script.c) in cyrus-imapd in Cyrus IMAP Server 2.2.13 and 2.3.14 allows local users to execute arbitrary code and read or modify arbitrary messages via a crafted SIEVE script, related to the incorrect use of the sizeof operator for determining buffer length, combined with an integer signedness error.	cyrus-imapd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00182769
9690	CVE-2009-2625	Medium		Apache Xerces2 Java, as used in Sun Java Runtime Environment (JRE) in JDK and JRE 6 before Update 15 and JDK and JRE 5.0 before Update 20, and in other products, allows remote attackers to cause a denial of service (infinite loop and application hang) via malformed XML input, as demonstrated by the Codenomicon XML fuzzing framework.	Xerces	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00269025
9691	CVE-2009-2624	Medium		The huft_build function in inflate.c in gzip before 1.3.13 creates a hufts (aka huffman) table that is too small, which allows remote attackers to cause a denial of service (application crash or infinite loop) or possibly execute arbitrary code via a crafted archive. NOTE: this issue is caused by a CVE-2006-4334 regression.	gzip	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00197971
9692	CVE-2009-2584	High		Off-by-one error in the options_write function in drivers/misc/sgi-gru/gruprocfs.c in the SGI GRU driver in the Linux kernel 2.6.30.2 and earlier on ia64 and x86 platforms might allow local users to overwrite arbitrary memory locations and gain privileges via a crafted count argument, which triggers a stack-based buffer overflow.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175289
9693	CVE-2009-2474	Medium		neon before 0.28.6, when OpenSSL is used, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180263
9694	CVE-2009-2473	Medium		neon before 0.28.6, when expat is used, does not properly detect recursion during entity expansion, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document containing a large number of nested entity references, a similar issue to CVE-2003-1564.	neon	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180267
9695	CVE-2009-2446	High		Multiple format string vulnerabilities in the dispatch_command function in libmysqld/sql_parse.cc in mysqld in MySQL 4.0.0 through 5.0.83 allow remote authenticated users to cause a denial of service (daemon crash) and possibly have unspecified other impact via format string specifiers in a database name in a (1) COM_CREATE_DB or (2) COM_DROP_DB request. NOTE: some of these details are obtained from third party information.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00173953

	A	B	C	D	E	F	G	H	I	J	K	L	M
9696	CVE-2009-2417	High		lib/ssluse.c in cURL and libcurl 7.4 through 7.19.5, when OpenSSL is used, does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177758
9697	CVE-2009-2416	Medium		Multiple use-after-free vulnerabilities in libxml2 2.5.10, 2.6.16, 2.6.26, 2.6.27, and 2.6.32, and libxml 1.8.17, allow context-dependent attackers to cause a denial of service (application crash) via crafted (1) Notation or (2) Enumeration attribute types in an XML file, as demonstrated by the Codenomicon XML fuzzing framework.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177757
9698	CVE-2009-2414	Medium		Stack consumption vulnerability in libxml2 2.5.10, 2.6.16, 2.6.26, 2.6.27, and 2.6.32, and libxml 1.8.17, allows context-dependent attackers to cause a denial of service (application crash) via a large depth of element declarations in a DTD, related to a function recursion, as demonstrated by the Codenomicon XML fuzzing framework.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177757
9699	CVE-2009-2409	Medium		The NSS library before 3.12.3, as used in Firefox; GnuTLS before 2.6.4 and 2.7.4; OpenSSL 0.9.8 through 0.9.8k; and other products support MD2 with X.509 certificates, which might allow remote attackers to spoof certificates by using MD2 design flaws to generate a hash collision in less than brute-force time. NOTE: the scope of this issue is currently limited because the amount of computation required is still large.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175292
9700	CVE-2009-2408	High		Mozilla Firefox before 3.5 and NSS before 3.12.3 do not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.	nss.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00234642
9701	CVE-2009-2407	Medium		Heap-based buffer overflow in the parse_tag_3_packet function in fs/ecryptfs/keystore.c in the eCryptfs subsystem in the Linux kernel before 2.6.30.4 allows local users to cause a denial of service (system crash) or possibly gain privileges via vectors involving a crafted eCryptfs file, related to a large encrypted key size in a Tag 3 packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175293
9702	CVE-2009-2406	Medium		Stack-based buffer overflow in the parse_tag_11_packet function in fs/ecryptfs/keystore.c in the eCryptfs subsystem in the Linux kernel before 2.6.30.4 allows local users to cause a denial of service (system crash) or possibly gain privileges via vectors involving a crafted eCryptfs file, related to not ensuring that the key signature length in a Tag 11 packet is compatible with the key signature buffer size.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175296
9703	CVE-2009-2404	High		Heap-based buffer overflow in a regular-expression parser in Mozilla Network Security Services (NSS) before 3.12.3, as used in Firefox, Thunderbird, SeaMonkey, Evolution, Pidgin, and AOL Instant Messenger (AIM), allows remote SSL servers to cause a denial of service (application crash) or possibly execute arbitrary code via a long domain name in the subject's Common Name (CN) field of an X.509 certificate, related to the cert_TestHostName function.	nss	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177759
9704	CVE-2009-2347	High		Multiple integer overflows in inter-color spaces conversion tools in libtiff 3.8 through 3.8.2, 3.9, and 4.0 allow context-dependent attackers to execute arbitrary code via a TIFF image with large (1) width and (2) height values, which triggers a heap-based buffer overflow in the (a) cvt_whole_image function in tiff2rgba and (b) tiffcvt function in rgb2ycbcr.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00173952
9705	CVE-2009-2287	Medium		The kvm_arch_vcpu_ioctl_set_sregs function in the KVM in Linux kernel 2.6 before 2.6.30, when running on x86 systems, does not validate the page table root in a KVM_SET_SREGS call, which allows local users to cause a denial of service (crash or hang) via a crafted cr3 value, which triggers a NULL pointer dereference in the gfn_to_rmap function.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00173957
9706	CVE-2009-2285	Medium		Buffer underflow in the LZWDecodeCompat function in libtiff 3.8.2 allows context-dependent attackers to cause a denial of service (crash) via a crafted TIFF image, a different vulnerability than CVE-2008-2327.	libtiff	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00173959
9707	CVE-2009-2042	Medium		libpng before 1.2.37 does not properly parse 1-bit interlaced images with width values that are not divisible by 8, which causes libpng to include uninitialized bits in certain rows of a PNG file and might allow remote attackers to read portions of sensitive memory via out-of-bounds pixels in the file.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170563
9708	CVE-2009-1961	Low		The inode double locking code in fs/ocfs2/file.c in the Linux kernel 2.6.30 before 2.6.30-rc3, 2.6.27 before 2.6.27.24, 2.6.29 before 2.6.29.4, and possibly other versions down to 2.6.19 allows local users to cause a denial of service (prevention of file creation and removal) via a series of splice system calls that trigger a deadlock between the generic_file_splice_write, splice_from_pipe, and ocfs2_file_splice_write functions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170553
9709	CVE-2009-1956	Medium		Off-by-one error in the apr_brigade_vprintf function in Apache APR-util before 1.3.5 on big-endian platforms allows remote attackers to obtain sensitive information or cause a denial of service (application crash) via crafted input.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170558

	A	B	C	D	E	F	G	H	I	J	K	L	M
9710	CVE-2009-1955	Medium		The expat XML parser in the apr_xml_* interface in xml/apr_xml.c in Apache APR-util before 1.3.7, as used in the mod_dav and mod_dav_svn modules in the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via a crafted XML document containing a large number of nested entity references, as demonstrated by a PROPFIND request, a similar issue to CVE-2003-1564.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170561
9711	CVE-2009-1932	Medium		Multiple integer overflows in the (1) user_info_callback, (2) user_endrow_callback, and (3) gst_pngdec_task functions (ext/libpng/gstpngdec.c) in GStreamer Good Plug-ins (aka gst-plugins-good or gstreamer-plugins-good) 0.10.15 allow remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted PNG file, which triggers a buffer overflow.	GStreamer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170552
9712	CVE-2009-1914	Medium		The pci_register_iommu_region function in arch/sparc/kernel/pci_common.c in the Linux kernel before 2.6.29 on the sparc64 platform allows local users to cause a denial of service (system crash) by reading the /proc/iomem file, related to uninitialized pointers and the request_resource function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170556
9713	CVE-2009-1904	Medium		The BigDecimal library in Ruby 1.8.6 before p369 and 1.8.7 before p173 allows context-dependent attackers to cause a denial of service (application crash) via a string argument that represents a large number, as demonstrated by an attempted conversion to the Float data type.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170554
9714	CVE-2009-1897	Medium		The tun_chr_poll function in drivers/net/tun.c in the tun subsystem in the Linux kernel 2.6.30 and 2.6.30.1, when the -fno-delete-null-pointer-checks gcc option is omitted, allows local users to gain privileges via vectors involving a NULL pointer dereference and an mmap of /dev/net/tun, a different vulnerability than CVE-2009-1894.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175295
9715	CVE-2009-1895	High		The personality subsystem in the Linux kernel before 2.6.31-rc3 has a PER_CLEAR_ON_SETID setting that does not clear the ADDR_COMPAT_LAYOUT and MMAP_PAGE_ZERO flags when executing a setuid or setgid program, which makes it easier for local users to leverage the details of memory usage to (1) conduct NULL pointer dereference attacks, (2) bypass the mmap_min_addr protection mechanism, or (3) defeat address space layout randomization (ASLR).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175291
9716	CVE-2009-1894	High		Race condition in PulseAudio 0.9.9, 0.9.10, and 0.9.14 allows local users to gain privileges via vectors involving creation of a hard link, related to the application setting LD_BIND_NOW to 1, and then calling execv on the target of the /proc/self/exe symlink.	PulseAudio	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175287
9717	CVE-2009-1893	Medium		The configtest function in the Red Hat dhcpd init script for DHCP 3.0.1 in Red Hat Enterprise Linux (RHEL) 3 allows local users to overwrite arbitrary files via a symlink attack on an unspecified temporary file, related to the dhcpd -t command.	dhcp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175286
9718	CVE-2009-1892	Medium		dhcpd in ISC DHCP 3.0.4 and 3.1.1, when the dhcp-client-identifier and hardware ethernet configuration settings are both used, allows remote attackers to cause a denial of service (daemon crash) via unspecified requests.	dhcp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175288
9719	CVE-2009-1891	Medium		The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00173955
9720	CVE-2009-1890	Medium		The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00173956
9721	CVE-2009-1888	Medium		The acl_group_override function in smbd/posix_acls.c in smbd in Samba 3.0.x before 3.0.35, 3.1.x and 3.2.x before 3.2.13, and 3.3.x before 3.3.6, when dos filemode is enabled, allows remote attackers to modify access control lists for files via vectors related to read access to uninitialized memory.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00172311
9722	CVE-2009-1887	Medium		agent/snmp_agent.c in snmpd in net-snmp 5.0.9 in Red Hat Enterprise Linux (RHEL) 3 allows remote attackers to cause a denial of service (daemon crash) via a crafted SNMP GETBULK request that triggers a divide-by-zero error. NOTE: this vulnerability exists because of an incorrect fix for CVE-2008-4309.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00172306
9723	CVE-2009-1886	High		Multiple format string vulnerabilities in client/client.c in smbclient in Samba 3.2.0 through 3.2.12 might allow context-dependent attackers to execute arbitrary code via format string specifiers in a filename.	samba	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00172309
9724	CVE-2009-1885	High		Stack consumption vulnerability in validators/DTD/DTDScanner.cpp in Apache Xerces C++ 2.7.0 and 2.8.0 allows context-dependent attackers to cause a denial of service (application crash) via vectors involving nested parentheses and invalid byte values in simply nested DTD structures, as demonstrated by the Codenomicon XML fuzzing framework.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00177760
9725	CVE-2009-1884	Medium		Off-by-one error in the bzinflate function in Bzip2.xs in the Compress-Raw-Bzip2 module before 2.018 for Perl allows context-dependent attackers to cause a denial of service (application hang or crash) via a crafted bzip2 compressed stream that triggers a buffer overflow, a related issue to CVE-2009-1391.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00180261

	A	B	C	D	E	F	G	H	I	J	K	L	M
9726	CVE-2009-1883	Medium		The z90crypt_unlocked_ioctl function in the z90crypt driver in the Linux kernel 2.6.9 does not perform a capability check for the Z90QUIESCE operation, which allows local users to leverage euid 0 privileges to force a driver outage.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00185834
9727	CVE-2009-1882	High		Integer overflow in the XMakeImage function in magick/xwindow.c in ImageMagick 6.5.2-8 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted TIFF file, which triggers a buffer overflow. NOTE: some of these details are obtained from third party information.	ImageMagick	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170564
9728	CVE-2009-1633	High		Multiple buffer overflows in the cifs subsystem in the Linux kernel before 2.6.29.4 allow remote CIFS servers to cause a denial of service (memory corruption) and possibly have unspecified other impact via (1) a malformed Unicode string, related to Unicode string area alignment in fs/cifs/sess.c; or (2) long Unicode characters, related to fs/cifs/cifssmb.c and the cifs_readdir function in fs/cifs/readdir.c.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00169091
9729	CVE-2009-1632	Medium		Multiple memory leaks in Ipsec-tools before 0.7.2 allow remote attackers to cause a denial of service (memory consumption) via vectors involving (1) signature verification during user authentication with X.509 certificates, related to the eay_check_x509sign function in src/racoon/crypto_openssl.c; and (2) the NAT-Traversal (aka NAT-T) keepalive implementation, related to src/racoon/nattraversal.c.	Ipsec-tools	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00167306
9730	CVE-2009-1630	Medium		The nfs_permission function in fs/nfs/dir.c in the NFS client implementation in the Linux kernel 2.6.29.3 and earlier, when atomic_open is available, does not check execute (aka EXEC or MAY_EXEC) permission bits, which allows local users to bypass permissions and execute files, as demonstrated by files on an NFSv4 fileserver.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00167304
9731	CVE-2009-1574	Medium		racoon/isakmp_frag.c in ipsec-tools before 0.7.2 allows remote attackers to cause a denial of service (crash) via crafted fragmented packets without a payload, which triggers a NULL pointer dereference.	Ipsec-tools	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00167305
9732	CVE-2009-1572	Medium		The BGP daemon (bgpd) in Quagga 0.99.11 and earlier allows remote attackers to cause a denial of service (crash) via an AS path containing ASN elements whose string representation is longer than expected, which triggers an assert error.	quagga	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00167900
9733	CVE-2009-1527	Medium		Race condition in the ptrace_attach function in kernel/ptrace.c in the Linux kernel before 2.6.30-rc4 allows local users to gain privileges via a PTRACE_ATTACH ptrace call during an exec system call that is launching a setuid application, related to locking an incorrect cred_exec_mutex object.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00167301
9734	CVE-2009-1490	Medium		Heap-based buffer overflow in Sendmail before 8.13.2 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via a long X- header, as demonstrated by an X-Testing header.	sendmail	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00167303
9735	CVE-2009-1439	High		Buffer overflow in fs/cifs/connect.c in CIFS in the Linux kernel 2.6.29 and earlier allows remote attackers to cause a denial of service (crash) via a long nativeFileSystem field in a Tree Connect response to an SMB mount request.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165535
9736	CVE-2009-1438	High		Integer overflow in the CSoundFile::ReadMed function (src/load_med.cpp) in libmodplug before 0.8.6, as used in gstreamer-plugins and other products, allows context-dependent attackers to execute arbitrary code via a MED file with a crafted (1) song comment or (2) song name, which triggers a heap-based buffer overflow.	gstreamer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165534
9737	CVE-2009-1417	Medium		gnutls-cli in GnuTLS before 2.6.6 does not verify the activation and expiration times of X.509 certificates, which allows remote attackers to successfully present a certificate that is (1) not yet valid or (2) no longer valid, related to lack of time checks in the _gnutls_x509_verify_certificate function in lib/x509/verify.c in libgnutls_x509, as used by (a) Exim, (b) OpenLDAP, and (c) libsoup.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165616
9738	CVE-2009-1416	Medium		lib/gnutls_pk.c in libgnutls in GnuTLS 2.5.0 through 2.6.5 generates RSA keys stored in DSA structures, instead of the intended DSA keys, which might allow remote attackers to spoof signatures on certificates or have unspecified other impact by leveraging an invalid DSA key.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165529
9739	CVE-2009-1415	Medium		lib/pk-libgcrypt.c in libgnutls in GnuTLS before 2.6.6 does not properly handle invalid DSA signatures, which allows remote attackers to cause a denial of service (application crash) and possibly have unspecified other impact via a malformed DSA key that triggers a (1) free of an uninitialized pointer or (2) double free.	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165539
9740	CVE-2009-1391	Medium		Off-by-one error in the inflate function in Zlib.xs in Compress::Raw::Zlib Perl module before 2.017, as used in AMaViS, SpamAssassin, and possibly other products, allows context-dependent attackers to cause a denial of service (hang or crash) via a crafted zlib compressed stream that triggers a heap-based buffer overflow, as exploited in the wild by Trojan.Downloader-71014 in June 2009.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00172310
9741	CVE-2009-1390	Medium		Mutt 1.5.19, when linked against (1) OpenSSL (mutt_ssl.c) or (2) GnuTLS (mutt_ssl_gnutls.c), allows connections when only one TLS certificate in the chain is accepted instead of verifying the entire chain, which allows remote attackers to spoof trusted servers via a man-in-the-middle attack.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00172307
9742	CVE-2009-1389	High		Buffer overflow in the RTL8169 NIC driver (drivers/net/r8169.c) in the Linux kernel before 2.6.30 allows remote attackers to cause a denial of service (kernel memory corruption and crash) via a long packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00172308

	A	B	C	D	E	F	G	H	I	J	K	L	M
9743	CVE-2009-1388	Medium		The ptrace_start function in kernel/ptrace.c in the Linux kernel 2.6.18 does not properly handle simultaneous execution of the do_coredump function, which allows local users to cause a denial of service (deadlock) via vectors involving the ptrace system call and a coredumping thread.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00173954
9744	CVE-2009-1387	Medium		The dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL before 1.0.0 Beta 2 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence DTLS handshake message, related to a fragment bug.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170559
9745	CVE-2009-1386	Medium		ssl/s3_pkt.c in OpenSSL before 0.9.8i allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a DTLS ChangeCipherSpec packet that occurs before ClientHello.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170560
9746	CVE-2009-1385	High		Integer underflow in the e1000_clean_rx_irq function in drivers/net/e1000/e1000_main.c in the e1000 driver in the Linux kernel before 2.6.30-rc8, the e1000e driver in the Linux kernel, and Intel Wired Ethernet (aka e1000) before 7.5.5 allows remote attackers to cause a denial of service (panic) via a crafted frame size.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170555
9747	CVE-2009-1384	Medium		pam_krb5 2.2.14 through 2.3.4, as used in Red Hat Enterprise Linux (RHEL) 5, generates different password prompts depending on whether the user account exists, which allows remote attackers to enumerate valid usernames.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00169090
9748	CVE-2009-1379	Medium		Use-after-free vulnerability in the dtls1_retrieve_buffered_fragment function in ssl/d1_both.c in OpenSSL 1.0.0 Beta 2 allows remote attackers to cause a denial of service (openssl s_client crash) and possibly have unspecified other impact via a DTLS packet, as demonstrated by a packet from a server that uses a crafted server certificate.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00169093
9749	CVE-2009-1378	Medium		Multiple memory leaks in the dtls1_process_out_of_seq_message function in ssl/d1_both.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allow remote attackers to cause a denial of service (memory consumption) via DTLS records that (1) are duplicates or (2) have sequence numbers much greater than current sequence numbers, aka DTLS fragment handling memory leak.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00169095
9750	CVE-2009-1377	Medium		The dtls1_buffer_record function in ssl/d1_pkt.c in OpenSSL 0.9.8k and earlier 0.9.8 versions allows remote attackers to cause a denial of service (memory consumption) via a large series of future epoch DTLS records that are buffered in a queue, aka DTLS record buffer limitation bug.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00169089
9751	CVE-2009-1360	High		The __inet6_check_established function in net/ipv6/inet6_hashtables.c in the Linux kernel before 2.6.29, when Network Namespace Support (aka NET_NS) is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via vectors involving IPv6 packets.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165533
9752	CVE-2009-1341	Medium		Memory leak in the dequote_bytea function in quote.c in the DBD::Pg (aka DBD-Pg or libdbd-pg-perl) module before 2.0.0 for Perl allows context-dependent attackers to cause a denial of service (memory consumption) by fetching data with BYTEA columns.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165540
9753	CVE-2009-1338	Medium		The kill_something_info function in kernel/signal.c in the Linux kernel before 2.6.28 does not consider PID namespaces when processing signals directed to PID -1, which allows local users to bypass the intended namespace isolation, and send arbitrary signals to all processes in all namespaces, via a kill command.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165618
9754	CVE-2009-1337	Medium		The exit_notify function in kernel/exit.c in the Linux kernel before 2.6.30-rc1 does not restrict exit signals when the CAP_KILL capability is held, which allows local users to send an arbitrary signal to a process by running a program that modifies the exit_signal field and then uses an exec system call to launch a setuid application.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165620
9755	CVE-2009-1336	Medium		fs/nfs/client.c in the Linux kernel before 2.6.23 does not properly initialize a certain structure member that stores the maximum NFS filename length, which allows local users to cause a denial of service (OOPS) via a long filename, related to the encode_lookup function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165615
9756	CVE-2009-1299	Medium		The pa_make_secure_dir function in core-util.c in PulseAudio 0.9.10 and 0.9.19 allows local users to change the ownership and permissions of arbitrary files via a symlink attack on a /tmp/.esd-##### temporary file.	PulseAudio	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00202136
9757	CVE-2009-1298	High		The ip_frag_reasm function in ipv4/ip_fragment.c in Linux kernel 2.6.32-rc8, and possibly earlier versions, calls IP_INC_STATS_BH with an incorrect argument, which allows remote attackers to cause a denial of service (NULL pointer dereference and hang) via long IP packets, possibly related to the ip_defrag function.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00194770
9758	CVE-2009-1297	Medium		iscsi_discovery in open-iscsi in SUSE openSUSE 10.3 through 11.1 and SUSE Linux Enterprise (SLE) 10 SP2 and 11 allows local users to overwrite arbitrary files via a symlink attack on an unspecified temporary file that has a predictable name.	iscsi	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189678
9759	CVE-2009-1296	Low		The eCryptfs support utilities (ecryptfs-utils) 73-0ubuntu6.1 on Ubuntu 9.04 stores the mount passphrase in installation logs, which might allow local users to obtain access to the filesystem by reading the log files from disk. NOTE: the log files are only readable by root.	ecryptfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170557
9760	CVE-2009-1274	Medium		Integer overflow in the qt_error parse_trak_atom function in demuxers/demux_qt.c in xine-lib 1.1.16.2 and earlier allows remote attackers to execute arbitrary code via a Quicktime movie file with a large count value in an STTS atom, which triggers a heap-based buffer overflow.	xine	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163850

	A	B	C	D	E	F	G	H	I	J	K	L	M
9761	CVE-2009-1273	Medium		pam_ssh 1.92 and possibly other versions, as used when PAM is compiled with USE=ssh, generates different error messages depending on whether the username is valid or invalid, which makes it easier for remote attackers to enumerate usernames.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163749
9762	CVE-2009-1265	Medium		Integer overflow in rose_sendmsg (sys/net/af_rose.c) in the Linux kernel 2.6.24.4, and other versions before 2.6.30-rc1, might allow remote attackers to obtain sensitive information via a large length value, which causes garbage memory to be sent.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163745
9763	CVE-2009-1252	Medium		Stack-based buffer overflow in the crypto_recv function in ntp_crypto.c in ntpd in NTP before 4.2.4p7 and 4.2.5 before 4.2.5p74, when OpenSSL and autokey are enabled, allows remote attackers to execute arbitrary code via a crafted packet containing an extension field.	ntpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00169094
9764	CVE-2009-1243	Medium		net/ipv4/udp.c in the Linux kernel before 2.6.29.1 performs an unlocking step in certain incorrect circumstances, which allows local users to cause a denial of service (panic) by reading zero bytes from the /proc/net/udp file and unspecified other files, related to the udp seq_file infrastructure.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163744
9765	CVE-2009-1242	Medium		The vmx_set_msr function in arch/x86/kvm/vmx.c in the VMX implementation in the KVM subsystem in the Linux kernel before 2.6.29.1 on the i386 platform allows guest OS users to cause a denial of service (OOPS) by setting the EFER_LME (aka Long mode enable) bit in the Extended Feature Enable Register (EFER) model-specific register, which is specific to the x86_64 platform.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163953
9766	CVE-2009-1215	Low		Race condition in GNU screen 4.0.3 allows local users to create or overwrite arbitrary files via a symlink attack on the /tmp/screen-exchange temporary file.	screen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163853
9767	CVE-2009-1214	Medium		GNU screen 4.0.3 creates the /tmp/screen-exchange temporary file with world-readable permissions, which might allow local users to obtain sensitive session information.	screen	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163851
9768	CVE-2009-1195	Medium		The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00169092
9769	CVE-2009-1194	Medium		Integer overflow in the pango_glyph_string_set_size function in pango/glyphstring.c in Pango before 1.24 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long glyph string that triggers a heap-based buffer overflow, as demonstrated by a long document.location value in Firefox.	Pango	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00167299
9770	CVE-2009-1192	Medium		drivers/char/agp/generic.c in the agp subsystem in the Linux kernel before 2.6.30-rc3 does not zero out pages that may later be available to a user-space process, which allows local users to obtain sensitive information by reading these pages.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165619
9771	CVE-2009-1191	Medium		mod_proxy_ajp.c in the mod_proxy_ajp module in the Apache HTTP Server 2.2.11 allows remote attackers to obtain sensitive response data, intended for a client that sent an earlier POST request with no request body, via an HTTP request.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165536
9772	CVE-2009-1186	Low		Buffer overflow in the util_path_encode function in udev/lib/libudev-util.c in udev before 1.4.1 allows local users to cause a denial of service (service outage) via vectors that trigger a call with crafted arguments.	udev	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165538
9773	CVE-2009-1185	High		udev before 1.4.1 does not verify whether a NETLINK message originates from kernel space, which allows local users to gain privileges by sending a NETLINK message from user space.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165621
9774	CVE-2009-1184	Medium		The selinux_ip_postroute_iptables_compat function in security/selinux/hooks.c in the SELinux subsystem in the Linux kernel before 2.6.27.22, and 2.6.28.x before 2.6.28.10, when compat_net is enabled, omits calls to avc_has_perm for the (1) node and (2) port, which allows local users to bypass intended restrictions on network traffic. NOTE: this was incorrectly reported as an issue fixed in 2.6.27.21.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00167300
9775	CVE-2009-1072	Medium		nfsd in the Linux kernel before 2.6.28.9 does not drop the CAP_MKNOD capability before handling a user request in a thread, which allows local users to create device nodes, as demonstrated on a filesystem that has been exported with the root_squash option.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163748
9776	CVE-2009-1046	Medium		The console selection feature in the Linux kernel 2.6.28 before 2.6.28.4, 2.6.25, and possibly earlier versions, when the UTF-8 console is used, allows physically proximate attackers to cause a denial of service (memory corruption) by selecting a small number of 3-byte UTF-8 characters, which triggers an an off-by-two memory error. NOTE: it is not clear whether this issue crosses privilege boundaries.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163957
9777	CVE-2009-0946	High		Multiple integer overflows in FreeType 2.3.9 and earlier allow remote attackers to execute arbitrary code via vectors related to large values in certain inputs in (1) smooth/ftsmooth.c, (2) sfnt/ttcmap.c, and (3) cff/cffload.c.	freetype	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165617
9778	CVE-2009-0935	Medium		The inotify_read function in the Linux kernel 2.6.27 to 2.6.27.13, 2.6.28 to 2.6.28.2, and 2.6.29-rc3 allows local users to cause a denial of service (OOPS) via a read with an invalid address to an inotify instance, which causes the device's event list mutex to be unlocked twice and prevents proper synchronization of a data structure for the inotify instance.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163858

	A	B	C	D	E	F	G	H	I	J	K	L	M
9779	CVE-2009-0922	Medium		PostgreSQL before 8.3.7, 8.2.13, 8.1.17, 8.0.21, and 7.4.25 allows remote authenticated users to cause a denial of service (stack consumption and crash) by triggering a failure in the conversion of a localized error message to a client-specified encoding, as demonstrated using mismatched encoding conversion requests.Per: https://bugzilla.redhat.com/show_bug.cgi?id=488156 PostgreSQL allows remote authenticated users to cause a momentary denial of service (crash due to stack consumption) when there is a failure to convert a localized error message to the client-specified encoding. In releases 8.3.6, 8.2.12, 8.1.16. 8.0.20, and 7.4.24, a trivial misconfiguration is sufficient to provoke a crash. In older releases it is necessary to select a locale and client encoding for which specific messages fail to translate, and so a given installation may or may not be vulnerable depending on the administrator-determined locale setting. Releases 8.3.7, 8.2.13, 8.1.17, 8.0.21, and 7.4.25 are secure against all known variants of this issue.	postgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163952
9780	CVE-2009-0887	Medium		Integer signedness error in the _pam_StrTok function in libpam/pam_misc.c in Linux-PAM (aka pam) 1.0.3 and earlier, when a configuration file contains non-ASCII usernames, might allow remote attackers to cause a denial of service, and might allow remote authenticated users to obtain login access with a different user's non-ASCII username, via a login attempt.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00160590
9781	CVE-2009-0859	Medium		The shm_get_stat function in ipc/shm.c in the shm subsystem in the Linux kernel before 2.6.28.5, when CONFIG_SHMEM is disabled, misinterprets the data type of an inode, which allows local users to cause a denial of service (system hang) via an SHM_INFO shmctl call, as demonstrated by running the ipcs program.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00160631
9782	CVE-2009-0848	Medium		Untrusted search path vulnerability in GTK2 in OpenSUSE 11.0 and 11.1 allows local users to execute arbitrary code via a Trojan horse GTK module in an unspecified relative search path.	gtk	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00160591
9783	CVE-2009-0847	Medium		The asn1buf_imbed function in the ASN.1 decoder in MIT Kerberos 5 (aka krb5) 1.6.3, when PK-INIT is used, allows remote attackers to cause a denial of service (application crash) via a crafted length value that triggers an erroneous malloc call, related to incorrect calculations with pointer arithmetic.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163854
9784	CVE-2009-0846	High		The asn1_decode_generaltime function in lib/krb5/asn.1/asn1_decode.c in the ASN.1 GeneralizedTime decoder in MIT Kerberos 5 (aka krb5) before 1.6.4 allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via vectors involving an invalid DER encoding that triggers a free of an uninitialized pointer.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163739
9785	CVE-2009-0845	Medium		The spnego_gss_accept_sec_context function in lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) 1.5 through 1.6.3, when SPNEGO is used, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via invalid ContextFlags data in the reqFlags field in a negTokenInit token.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163743
9786	CVE-2009-0844	Medium		The get_input_token function in the SPNEGO implementation in MIT Kerberos 5 (aka krb5) 1.5 through 1.6.3 allows remote attackers to cause a denial of service (daemon crash) and possibly obtain sensitive information via a crafted length value that triggers a buffer over-read.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163742
9787	CVE-2009-0835	High		The __secure_computing function in kernel/seccomp.c in the seccomp subsystem in the Linux kernel 2.6.28.7 and earlier on the x86_64 platform, when CONFIG_SECCOMP is enabled, does not properly handle (1) a 32-bit process making a 64-bit syscall or (2) a 64-bit process making a 32-bit syscall, which allows local users to bypass intended access restrictions via crafted syscalls that are misinterpreted as (a) stat or (b) chmod, a related issue to CVE-2009-0342 and CVE-2009-0343.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00160630
9788	CVE-2009-0834	High		The audit_syscall_entry function in the Linux kernel 2.6.28.7 and earlier on the x86_64 platform does not properly handle (1) a 32-bit process making a 64-bit syscall or (2) a 64-bit process making a 32-bit syscall, which allows local users to bypass certain syscall audit configurations via crafted syscalls, a related issue to CVE-2009-0342 and CVE-2009-0343.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00160589
9789	CVE-2009-0819	Medium		sql/item_xmlfunc.cc in MySQL 5.1 before 5.1.32 and 6.0 before 6.0.10 allows remote authenticated users to cause a denial of service (crash) via an XPath expression employing a scalar expression as a FilterExpr with ExtractValue() or UpdateXML(), which triggers an assertion failure.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00160632
9790	CVE-2009-0798	Medium		The daemon in acpid before 1.0.10 allows remote attackers to cause a denial of service (CPU consumption and connectivity loss) by opening a large number of UNIX sockets without closing them, which triggers an infinite loop.	acpid	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165532
9791	CVE-2009-0796	Low		Cross-site scripting (XSS) vulnerability in Status.pm in Apache::Status and Apache2::Status in mod_perl1 and mod_perl2 for the Apache HTTP Server, when /perl-status is accessible, allows remote attackers to inject arbitrary web script or HTML via the URI.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163849

	A	B	C	D	E	F	G	H	I	J	K	L	M
9792	CVE-2009-0790	Medium		The pluto IKE daemon in Openswan and Strongswan IPsec 2.6 before 2.6.21 and 2.4 before 2.4.14, and Strongswan 4.2 before 4.2.14 and 2.8 before 2.8.9, allows remote attackers to cause a denial of service (daemon crash and restart) via a crafted (1) R_U_THERE or (2) R_U_THERE_ACK Dead Peer Detection (DPD) IPsec IKE Notification message that triggers a NULL pointer dereference related to inconsistent ISAKMP state and the lack of a phase2 state association in DPD.	IPsec	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163741
9793	CVE-2009-0789	Medium		OpenSSL before 0.9.8k on WIN64 and certain other platforms does not properly handle a malformed ASN.1 structure, which allows remote attackers to cause a denial of service (invalid memory access and application crash) by placing this structure in the public key of a certificate, as demonstrated by an RSA public key.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163950
9794	CVE-2009-0787	Medium		The ecryptfs_write_metadata_to_contents function in the eCryptfs functionality in the Linux kernel 2.6.28 before 2.6.28.9 uses an incorrect size when writing kernel memory to an eCryptfs file header, which triggers an out-of-bounds read and allows local users to obtain portions of kernel memory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163857
9795	CVE-2009-0778	High		The icmp_send function in net/ipv4/icmp.c in the Linux kernel before 2.6.25, when configured as a router with a REJECT route, does not properly manage the Protocol Independent Destination Cache (aka DST) in some situations involving transmission of an ICMP Host Unreachable message, which allows remote attackers to cause a denial of service (connectivity outage) by sending a large series of packets to many destination IP addresses within this REJECT route, related to an rt_cache leak.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00160588
9796	CVE-2009-0748	Medium		The ext4_fill_super function in fs/ext4/super.c in the Linux kernel 2.6.27 before 2.6.27.19 and 2.6.28 before 2.6.28.7 does not validate the superblock configuration, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) by attempting to mount a crafted ext4 filesystem.	WRLinux doesn't ship EXT4.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159329
9797	CVE-2009-0747	Medium		The ext4_isize function in fs/ext4/ext4.h in the Linux kernel 2.6.27 before 2.6.27.19 and 2.6.28 before 2.6.28.7 uses the i_size_high structure member during operations on arbitrary types of files, which allows local users to cause a denial of service (CPU consumption and error-message flood) by attempting to mount a crafted ext4 filesystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158992
9798	CVE-2009-0746	Medium		The make_indexed_dir function in fs/ext4/namei.c in the Linux kernel 2.6.27 before 2.6.27.19 and 2.6.28 before 2.6.28.7 does not validate a certain rec_len field, which allows local users to cause a denial of service (OOPS) by attempting to mount a crafted ext4 filesystem.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159242
9799	CVE-2009-0745	Medium		The ext4_group_add function in fs/ext4/resize.c in the Linux kernel 2.6.27 before 2.6.27.19 and 2.6.28 before 2.6.28.7 does not properly initialize the group descriptor during a resize (aka resize2fs) operation, which might allow local users to cause a denial of service (OOPS) by arranging for crafted values to be present in available memory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158996
9800	CVE-2009-0696	Medium		The dns_db_findrdataset function in db.c in named in ISC BIND 9.4 before 9.4.3-P3, 9.5 before 9.5.1-P3, and 9.6 before 9.6.1-P1, when configured as a master server, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via an ANY record in the prerequisite section of a crafted dynamic update message, as exploited in the wild in July 2009.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00175290
9801	CVE-2009-0692	High		Stack-based buffer overflow in the script_write_params method in client/dhclient.c in ISC DHCP dhclient 4.1 before 4.1.0p1, 4.0 before 4.0.1p1, 3.1 before 3.1.2p1, 3.0, and 2.0 allows remote DHCP servers to execute arbitrary code via a crafted subnet-mask option.	dhcp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00173958
9802	CVE-2009-0688	High		Multiple buffer overflows in the CMU Cyrus SASL library before 2.1.23 might allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via strings that are used as input to the sasl_encode64 function in lib/saslutil.c.	cyrus-sasl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00167302
9803	CVE-2009-0676	Low		The sock_getsockopt function in net/core/sock.c in the Linux kernel before 2.6.28.6 does not initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel memory via an SO_BSDCOMPAT getsockopt request.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158990
9804	CVE-2009-0675	Low		The skfp_ioctl function in drivers/net/skfp/skfddi.c in the Linux kernel before 2.6.28.6 permits SKFP_CLR_STATS requests only when the CAP_NET_ADMIN capability is absent, instead of when this capability is present, which allows local users to reset the driver statistics, related to an inverted logic issue.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159066
9805	CVE-2009-0663	High		Heap-based buffer overflow in the DBD::Pg (aka DBD-Pg or libdbd-pg-perl) module 1.49 for Perl might allow context-dependent attackers to execute arbitrary code via unspecified input to an application that uses the getline and pg_getline functions to read database rows.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165537
9806	CVE-2009-0653	Medium		OpenSSL, probably 0.9.6, does not verify the Basic Constraints for an intermediate CA-signed certificate, which allows remote attackers to spoof the certificates of trusted sites via a man-in-the-middle attack, a related issue to CVE-2002-0970.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158995
9807	CVE-2009-0642	Medium		ext/openssl/ossl_ocsp.c in Ruby 1.8 and 1.9 does not properly check the return value from the OCSP_basic_verify function, which might allow remote attackers to successfully present an invalid X.509 certificate, possibly involving a revoked certificate.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159150

	A	B	C	D	E	F	G	H	I	J	K	L	M
9808	CVE-2009-0605	Medium		Stack consumption vulnerability in the do_page_fault function in arch/x86/mm/fault.c in the Linux kernel before 2.6.28.5 allows local users to cause a denial of service (memory corruption) or possibly gain privileges via unspecified vectors that trigger page faults on a machine that has a registered Kprobes probe.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159072
9809	CVE-2009-0591	Low		The CMS_verify function in OpenSSL 0.9.8h through 0.9.8j, when CMS is enabled, does not properly handle errors associated with malformed signed attributes, which allows remote attackers to repudiate a signature that originally appeared to be valid but was actually invalid.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163955
9810	CVE-2009-0590	Medium		The ASN1_STRING_print_ex function in OpenSSL before 0.9.8k allows remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a (1) BMPString or (2) UniversalString with an invalid encoded length.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163950
9811	CVE-2009-0586	Medium		Integer overflow in gst-libs/gst/tag/gstvorbistag.c in vorbistag in gst-plugins-base (aka gstreamer-plugins-base) before 0.10.23 in GStreamer allows context-dependent attackers to execute arbitrary code via a long string that is converted from a base64 representation.	Gstreamer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163740
9812	CVE-2009-0579	Medium		Linux-PAM before 1.0.4 does not enforce the minimum password age (MINDAYS) as specified in /etc/shadow, which allows local users to bypass intended security policy and change their passwords sooner than specified.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00165622
9813	CVE-2009-0398	High		Array index error in the gst_qtp_trak_handler function in gst/qtdemux/qtdemux.c in GStreamer Plug-ins (aka gstreamer-plugins) 0.6.0 allows remote attackers to have an unknown impact via a crafted QuickTime media file.	Gstreamer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163746
9814	CVE-2009-0397	High		Heap-based buffer overflow in the qtdemux_parse_samples function in gst/qtdemux/qtdemux.c in GStreamer Good Plug-ins (aka gst-plugins-good) 0.10.9 through 0.10.11, and GStreamer Plug-ins (aka gstreamer-plugins) 0.8.5, might allow remote attackers to execute arbitrary code via crafted Time-to-sample (aka stts) atom data in a malformed QuickTime media .mov file.	Gstreamer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163747
9815	CVE-2009-0387	High		Array index error in the qtdemux_parse_samples function in gst/qtdemux/qtdemux.c in GStreamer Good Plug-ins (aka gst-plugins-good) 0.10.9 through 0.10.11 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via crafted Sync Sample (aka stss) atom data in a malformed QuickTime media .mov file, related to mark keyframes.	GStreamer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163856
9816	CVE-2009-0386	High		Heap-based buffer overflow in the qtdemux_parse_samples function in gst/qtdemux/qtdemux.c in GStreamer Good Plug-ins (aka gst-plugins-good) 0.10.9 through 0.10.11 might allow remote attackers to execute arbitrary code via crafted Composition Time To Sample (ctts) atom data in a malformed QuickTime media .mov file.	GStreamer	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163859
9817	CVE-2009-0361	Medium		Russ Allbery pam-krb5 before 3.13, as used by libpam-heimdal, su in Solaris 10, and other software, does not properly handle calls to pam_setcred when running setuid, which allows local users to overwrite and change the ownership of arbitrary files by setting the KRB5CCNAME environment variable, and then launching a setuid application that performs certain pam_setcred operations.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156649
9818	CVE-2009-0360	Medium		Russ Allbery pam-krb5 before 3.13, when linked against MIT Kerberos, does not properly initialize the Kerberos libraries for setuid use, which allows local users to gain privileges by pointing an environment variable to a modified Kerberos configuration file, and then launching a PAM-based setuid application.Per vendor advisory: http://www.eyrie.org/~eagle/software/pam-krb5/security/2009-02-11.html This advisory is only for my pam-krb5 module, as distributed from my web site and packaged by Debian, Ubuntu, and Gentoo.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156599
9819	CVE-2009-0322	Medium		drivers/firmware/dell_rbu.c in the Linux kernel before 2.6.27.13, and 2.6.28.x before 2.6.28.2, allows local users to cause a denial of service (system crash) via a read system call that specifies zero bytes from the (1) image_type or (2) packet_size file in /sys/devices/platform/dell_rbu/.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154980
9820	CVE-2009-0316	Medium		Untrusted search path vulnerability in the Python module in vim allows local users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	VIM	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154907
9821	CVE-2009-0269	Medium		fs/ecryptfs/inode.c in the eCryptfs subsystem in the Linux kernel before 2.6.28.1 allows local users to cause a denial of service (fault or memory corruption), or possibly have unspecified other impact, via a readlink call that results in an error, leading to use of a -1 return value as an array index.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154950
9822	CVE-2009-0265	Medium		Internet Systems Consortium (ISC) BIND 9.6.0 and earlier does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077 and CVE-2009-0025.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154946
9823	CVE-2009-0180	High		Certain Fedora build scripts for nfs-utils before 1.1.2-9.fc9 on Fedora 9, and before 1.1.4-6.fc10 on Fedora 10, omit TCP Wrapper support, which might allow remote attackers to bypass intended access restrictions, possibly a related issue to CVE-2008-1376.	Nfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154962

	A	B	C	D	E	F	G	H	I	J	K	L	M
9824	CVE-2009-0159	Medium		Stack-based buffer overflow in the cookedprint function in ntpq/ntpq.c in ntpq in NTP before 4.2.4p7-RC2 allows remote NTP servers to execute arbitrary code via a crafted response.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163855
9825	CVE-2009-0129	Medium		libcrypt-openssl-dsa-perl does not properly check the return value from the OpenSSL DSA_verify and DSA_do_verify functions, which might allow remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00152470
9826	CVE-2009-0115	Medium		multipath-tools in SUSE openSUSE 10.3 through 11.0 and SUSE Linux Enterprise Server (SLES) 10 uses world-writable permissions for the socket file (aka /var/run/multipathd.sock), which allows local users to send arbitrary commands to the multipath daemon.	multipath	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163956
9827	CVE-2009-0065	High		Buffer overflow in net/sctp/sm_statefuns.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.28-git8 allows remote attackers to have an unknown impact via an FWD-TSN (aka FORWARD-TSN) chunk with a large stream ID.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00152432
9828	CVE-2009-0040	Medium		The PNG reference library (aka libpng) before 1.0.43, and 1.2.x before 1.2.35, as used in pngcrush and other applications, allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file that triggers a free of an uninitialized pointer in (1) the png_read_png function, (2) pCAL chunk handling, or (3) setup of 16-bit gamma tables.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158917
9829	CVE-2009-0037	Medium		The redirect implementation in curl and libcurl 5.11 through 7.19.3, when CURLOPT_FOLLOWLOCATION is enabled, accepts arbitrary Location values, which might allow remote HTTP servers to (1) trigger arbitrary requests to intranet servers, (2) read or overwrite arbitrary files via a redirect to a file: URL, or (3) execute arbitrary commands via a redirect to an scp: URL.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00160587
9830	CVE-2009-0034	Medium		parse.c in sudo 1.6.9p17 through 1.6.9p19 does not properly interpret a system group (aka %group) in the sudoers file during authorization decisions for a user who belongs to that group, which allows local users to leverage an applicable sudoers file and gain root privileges via a sudo command.	sudo	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154974
9831	CVE-2009-0031	Medium		Memory leak in the keyctl_join_session_keyring function (security/keys/keyctl.c) in Linux kernel 2.6.29-rc2 and earlier allows local users to cause a denial of service (kernel memory consumption) via unknown vectors related to a missing kfree.	Linux kernel 2.6.29-rc2 and earlier	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154911
9832	CVE-2009-0029	Medium		The ABI in the Linux kernel 2.6.28 and earlier on s390, powerpc, sparc64, and mips 64-bit platforms requires that a 32-bit argument in a 64-bit register was properly sign extended when sent from a user-mode application, but cannot verify this, which allows local users to cause a denial of service (crash) or possibly gain privileges via a crafted system call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00151797
9833	CVE-2009-0028	Medium		The clone system call in the Linux kernel 2.6.28 and earlier allows local users to send arbitrary signals to a parent process from an unprivileged child process by launching an additional child process with the CLONE_PARENT flag, and then letting this Unchanged process exit.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158922
9834	CVE-2009-0026	Medium		Multiple cross-site scripting (XSS) vulnerabilities in Apache Jackrabbit before 1.5.2 allow remote attackers to inject arbitrary web script or HTML via the q parameter to (1) search.jsp or (2) swr.jsp.	Apache Jackrabbit before 1.5.2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154908
9835	CVE-2009-0025	Medium		BIND 9.4.3 and earlier does not properly check the return value from the OpenSSL DSA_verify function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00152436
9836	CVE-2009-0024	High		The sys_remap_file_pages function in mm/fremap.c in the Linux kernel before 2.6.24.1 allows local users to cause a denial of service or gain privileges via unspecified vectors, related to the vm_file structure member, and the mmap_region and do_munmap functions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00152469
9837	CVE-2009-0023	Medium		The apr_strmatch_precompile function in strmatch/apr_strmatch.c in Apache APR-util before 1.3.5 allows remote attackers to cause a denial of service (daemon crash) via crafted input involving (1) a .htaccess file used with the Apache HTTP Server, (2) the SVNMasterURI directive in the mod_dav_svn module in the Apache HTTP Server, (3) the mod_apreq2 module for the Apache HTTP Server, or (4) an application that uses the libapreq2 library, related to an underflow flaw.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00170562
9838	CVE-2009-0021	Medium		NTP 4.2.4 before 4.2.4p5 and 4.2.5 before 4.2.5p150 does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys, a similar vulnerability to CVE-2008-5077.Note that versions 4.2.5 before 4.2.5p150 are development versions and not production versions. Development versions are not included in the CPE configuration for CVEs.	ntp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00152463
9839	CVE-2008-7316	Low		mm/filemap.c in the Linux kernel before 2.6.25 allows local users to cause a denial of service (infinite loop) via a writev system call that triggers an iovec of zero length, followed by a page fault for an iovec of nonzero length.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-626

	A	B	C	D	E	F	G	H	I	J	K	L	M
9840	CVE-2008-7270	Medium		OpenSSL before 0.9.8j, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG is enabled, does not prevent modification of the ciphersuite in the session cache, which allows remote attackers to force the use of a disabled cipher via vectors involving sniffing network traffic to discover a session identifier, a different vulnerability than CVE-2010-4180.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00247364
9841	CVE-2008-7256	Low		mm/shmem.c in the Linux kernel before 2.6.28-rc8, when strict overcommit is enabled and CONFIG_SECURITY is disabled, does not properly handle the export of shmemfs objects by knfsd, which allows attackers to cause a denial of service (NULL pointer dereference and knfsd crash) or possibly have unspecified other impact via unknown vectors. NOTE: this vulnerability exists because of an incomplete fix for CVE-2010-1643.	linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218805
9842	CVE-2008-7247	Medium		sql/sql_table.cc in MySQL 5.0.x through 5.0.88, 5.1.x through 5.1.41, and 6.0 before 6.0.9-alpha, when the data home directory contains a symlink to a different filesystem, allows remote authenticated users to bypass intended access restrictions by calling CREATE TABLE with a (1) DATA DIRECTORY or (2) INDEX DIRECTORY argument referring to a subdirectory that requires following this symlink.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00193779
9843	CVE-2008-7177	High		Buffer overflow in the listing module in Netwide Assembler (NASM) before 2.03.01 has unknown impact and attack vectors, a different vulnerability than CVE-2008-2719.	NASM	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00182770
9844	CVE-2008-6235	High		The Netrw plugin (netrw.vim) in Vim 7.0 and 7.1 allows user-assisted attackers to execute arbitrary commands via shell metacharacters in a filename used by the (1) D (delete) command or (2) b:netrw_curdir variable, as demonstrated using the netrw.v4 and netrw.v5 test cases.	vim	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159238
9845	CVE-2008-6218	High		Memory leak in the png_handle_tEXt function in pngrutil.c in libpng before 1.2.33 rc02 and 1.4.0 beta36 allows context-dependent attackers to cause a denial of service (memory exhaustion) via a crafted PNG file.	libpng before 1.2.33 rc02 and 1.4.0 beta36	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158997
9846	CVE-2008-6123	Medium		The netsnmp_udp_fmtaddr function (snmplib/snmpUDPDomain.c) in net-snmp 5.0.9 through 5.4.2, when using TCP wrappers for client authorization, does not properly parse hosts.allow rules, which allows remote attackers to bypass intended access restrictions and execute SNMP queries, related to source/destination IP address confusion.	Net-snmp 5.0.9 through 5.4.2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156613
9847	CVE-2008-6107	Medium		The (1) sys32_mremap function in arch/sparc64/kernel/sys_sparc32.c, the (2) sparc_mmap_check function in arch/sparc/kernel/sys_sparc.c, and the (3) sparc64_mmap_check function in arch/sparc64/kernel/sys_sparc.c, in the Linux kernel before 2.6.25.4, omit some virtual-address range (aka span) checks when the mremap MREMAP_FIXED bit is not set, which allows local users to cause a denial of service (panic) via unspecified mremap calls, a related issue to CVE-2008-2137.	Linux kernel before 2.6.25.4	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156606
9848	CVE-2008-5983	Medium		Untrusted search path vulnerability in the PySys_SetArgv API function in Python before 2.6 prepends an empty string to sys.path when the argv[0] argument does not contain a path separator, which might allow local users to execute arbitrary code via a Trojan horse Python file in the current working directory.	Python before 2.6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154939
9849	CVE-2008-5907	Medium		The png_check_keyword function in pngwutil.c in libpng before 1.0.42, and 1.2.x before 1.2.34, might allow context-dependent attackers to set the value of an arbitrary memory location to zero via vectors involving creation of crafted PNG files with keywords, related to an implicit cast of the '\0' character constant to a NULL pointer. NOTE: some sources incorrectly report this as a double free vulnerability.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00152448
9850	CVE-2008-5714	High		Off-by-one error in monitor.c in Qemu 0.9.1 might make it easier for remote attackers to guess the VNC password, which is limited to seven characters where eight was intended.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00150981
9851	CVE-2008-5713	Medium		The __qdisc_run function in net/sched/sch_generic.c in the Linux kernel before 2.6.25 on SMP machines allows local users to cause a denial of service (soft lockup) by sending a large amount of network traffic, as demonstrated by multiple simultaneous invocations of the Netperf benchmark application in UDP_STREAM mode.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00150968
9852	CVE-2008-5702	High		Buffer underflow in the ibwdt_ioctl function in drivers/watchdog/ib700wdt.c in the Linux kernel before 2.6.28-rc1 might allow local users to have an unknown impact via a certain /dev/watchdog WDIOC_SETTIMEOUT IOCTL call.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00150998
9853	CVE-2008-5701	Medium		Array index error in arch/mips/kernel/scall64-o32.S in the Linux kernel before 2.6.28-rc8 on 64-bit MIPS platforms allows local users to cause a denial of service (system crash) via an o32 syscall with a small syscall number, which leads to an attempted read operation outside the bounds of the syscall table.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00151014
9854	CVE-2008-5700	Medium		libata in the Linux kernel before 2.6.27.9 does not set minimum timeouts for SG_IO requests, which allows local users to cause a denial of service (Programmed I/O mode on drives) via multiple simultaneous invocations of an unspecified test program.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00150971
9855	CVE-2008-5676	Medium		Multiple unspecified vulnerabilities in the ModSecurity (aka mod_security) module 2.5.0 through 2.5.5 for the Apache HTTP Server, when SecCacheTransformations is enabled, allow remote attackers to cause a denial of service (daemon crash) or bypass the product's functionality via unknown vectors related to transformation caching.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00150969

	A	B	C	D	E	F	G	H	I	J	K	L	M
9856	CVE-2008-5519	Low		The JK Connector (aka mod_jk) 1.2.0 through 1.2.26 in Apache Tomcat allows remote attackers to obtain sensitive information via an arbitrary request from an HTTP client, in opportunistic circumstances involving (1) a request from a different client that included a Content-Length header but no POST data or (2) a rapid series of requests, related to noncompliance with the AJP protocol's requirements for requests containing Content-Length headers.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163852
9857	CVE-2008-5395	Medium		The parisc_show_stack function in arch/parisc/kernel/traps.c in the Linux kernel before 2.6.28-rc7 on PA-RISC allows local users to cause a denial of service (system crash) via vectors associated with an attempt to unwind a stack that contains userspace addresses.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149274
9858	CVE-2008-5394	High		/bin/login in shadow 4.0.18.1 in Debian GNU/Linux, and probably other Linux distributions, allows local users in the utmp group to overwrite arbitrary files via a symlink attack on a temporary file referenced in a line (aka ut_line) field in a utmp entry.	shadow	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149284
9859	CVE-2008-5374	Medium		bash-doc 3.2 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/cb#####.? temporary file, related to the (1) aliasconv.sh, (2) aliasconv.bash, and (3) cshtobash scripts.	bash	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149277
9860	CVE-2008-5367	Medium		ip-up in ppp-udeb 2.4.4rel on Debian GNU/Linux allows local users to overwrite arbitrary files via a symlink attack on the /tmp/resolv.conf.tmp temporary file.	ppp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149328
9861	CVE-2008-5366	Medium		The postinst script in ppp 2.4.4rel on Debian GNU/Linux allows local users to overwrite arbitrary files via a symlink attack on the (1) /tmp/probe-finished or (2) /tmp/ppp-errors temporary file.	ppp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149276
9862	CVE-2008-5303	Medium		Race condition in the rmtree function in File::Path 1.08 (lib/File/Path.pm) in Perl 5.8.8 allows local users to allows local users to delete arbitrary files via a symlink attack, a different vulnerability than CVE-2005-0448, CVE-2004-0452, and CVE-2008-2827. NOTE: this is a regression error related to CVE-2005-0448. It is different from CVE-2008-5302 due to affected versions.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149322
9863	CVE-2008-5302	Medium		Race condition in the rmtree function in File::Path 1.08 and 2.07 (lib/File/Path.pm) in Perl 5.8.8 and 5.10.0 allows local users to create arbitrary setuid binaries via a symlink attack, a different vulnerability than CVE-2005-0448, CVE-2004-0452, and CVE-2008-2827. NOTE: this is a regression error related to CVE-2005-0448. It is different from CVE-2008-5303 due to affected versions.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149307
9864	CVE-2008-5300	Medium		Linux kernel 2.6.28 allows local users to cause a denial of service (soft lockup and process loss) via a large number of sendmsg function calls, which does not block during AF_UNIX garbage collection and triggers an OOM condition, a different vulnerability than CVE-2008-5029.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149329
9865	CVE-2008-5182	Medium		The inotify functionality in Linux kernel 2.6 before 2.6.28-rc5 might allow local users to gain privileges via unknown vectors related to race conditions in inotify watch removal and umount.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00146831
9866	CVE-2008-5161	Low		Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.http://securitytracker.com/alerts/2008/Nov/1021235.html CBC mode connections are affected	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00146880
9867	CVE-2008-5145	Medium		ltpmenu in ltp 20060918 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/runltp.mainmenu.##### temporary file.	ltp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00146846
9868	CVE-2008-5134	High		Buffer overflow in the lbs_process_bss function in drivers/net/wireless/libertas/scan.c in the libertas subsystem in the Linux kernel before 2.6.27.5 allows remote attackers to have an unknown impact via an invalid beacon/probe response.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00146872
9869	CVE-2008-5110	High		syslog-ng does not call chdir when it calls chroot, which might allow attackers to escape the intended jail. NOTE: this is only a vulnerability when a separate vulnerability is present.	Syslog-ng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00146863
9870	CVE-2008-5079	Medium		net/atm/svc.c in the ATM subsystem in the Linux kernel 2.6.27.8 and earlier allows local users to cause a denial of service (kernel infinite loop) by making two calls to svc_listen for the same socket, and then reading a /proc/net/atm/*vc file, related to corruption of the vcc table.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149297
9871	CVE-2008-5077	Medium		OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.	OpenSSL 0.9.8i and earlier	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00152429
9872	CVE-2008-5033	High		The chip_command function in drivers/media/video/tvaudio.c in the Linux kernel 2.6.25.x before 2.6.25.19, 2.6.26.x before 2.6.26.7, and 2.6.27.x before 2.6.27.3 allows attackers to cause a denial of service (NULL function pointer dereference and OOPS) via unknown vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144880

	A	B	C	D	E	F	G	H	I	J	K	L	M
9873	CVE-2008-5031	High		Multiple integer overflows in Python 2.5.2 allow context-dependent attackers to have an unknown impact via a large integer value in the tabsize argument to the expandtabs method, as implemented by (1) the string_expandtabs function in Objects/stringobject.c and (2) the unicode_expandtabs function in Objects/unicodeobject.c. NOTE: this vulnerability reportedly exists because of an incomplete fix for CVE-2008-2315.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144895
9874	CVE-2008-5029	Medium		The __scm_destroy function in net/core/scm.c in the Linux kernel 2.6.27.4, 2.6.26, and earlier makes indirect recursive calls to itself through calls to the fput function, which allows local users to cause a denial of service (panic) via vectors related to sending an SCM_RIGHTS message through a UNIX domain socket and closing file descriptors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144857
9875	CVE-2008-5025	High		Stack-based buffer overflow in the hfs_cat_find_brec function in fs/hfs/catalog.c in the Linux kernel before 2.6.28-rc1 allows attackers to cause a denial of service (memory corruption or system crash) via an hfs filesystem image with an invalid catalog namelength field, a related issue to CVE-2008-4933.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00146857
9876	CVE-2008-4989	Medium		The _gnutls_x509_verify_certificate function in lib/x509/verify.c in libgnutls in GnuTLS before 2.6.1 trusts certificate chains in which the last certificate is an arbitrary trusted, self-signed certificate, which allows man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).	gnutls	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144922
9877	CVE-2008-4968	Medium		The (1) rccs and (2) STUFF scripts in lmbench 3.0-a7 allow local users to overwrite arbitrary files via a symlink attack on a /tmp/sdiff.##### temporary file.	lmbench	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144898
9878	CVE-2008-4951	Medium		dtc 0.29.6 allows local users to overwrite arbitrary files via a symlink attack on (a) /tmp/awstats.log, (b) /tmp/spam.log.#####, and (c) /tmp/spam_err.log temporary files, related to the (1) accesslog.php and (2) sa-wrapper scripts.	dtc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144902
9879	CVE-2008-4934	High		The hfsplus_block_allocate function in fs/hfsplus/bitmap.c in the Linux kernel before 2.6.28-rc1 does not check a certain return value from the read_mapping_page function before calling kmap, which allows attackers to cause a denial of service (system crash) via a crafted hfsplus filesystem image.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144856
9880	CVE-2008-4933	High		Buffer overflow in the hfsplus_find_cat function in fs/hfsplus/catalog.c in the Linux kernel before 2.6.28-rc1 allows attackers to cause a denial of service (memory corruption or system crash) via an hfsplus filesystem image with an invalid catalog namelength field, related to the hfsplus_cat_build_key_uni function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144865
9881	CVE-2008-4864	High		Multiple integer overflows in imageop.c in the imageop module in Python 1.5.2 through 2.5.1 allow context-dependent attackers to break out of the Python VM and execute arbitrary code via large integer values in certain arguments to the crop function, leading to a buffer overflow, a different vulnerability than CVE-2007-4965 and CVE-2008-1679.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00142931
9882	CVE-2008-4832	Medium		rc.sysinit in initscripts 8.12-8.21 and 8.56.15-0.1 on rPath allows local users to delete arbitrary files via a symlink attack on a directory under (1) /var/lock or (2) /var/run. NOTE: this issue exists because of a race condition in an incorrect fix for CVE-2008-3524. NOTE: exploitation may require an unusual scenario in which rc.sysinit is executed other than at boot time.	initscripts	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00146837
9883	CVE-2008-4677	Medium		autoload/netrw.vim (aka the Netrw Plugin) 109, 131, and other versions before 133k for Vim 7.1.266, other 7.1 versions, and 7.2 stores credentials for an FTP session, and sends those credentials when attempting to establish subsequent FTP sessions to servers on different hosts, which allows remote FTP servers to obtain sensitive information in opportunistic circumstances by logging usernames and passwords. NOTE: the upstream vendor disputes a vector involving different ports on the same host, stating I'm assuming that they're using the same id and password on that unchanged hostname, deliberately.	vim	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00142943
9884	CVE-2008-4618	High		The Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.27 does not properly handle a protocol violation in which a parameter has an invalid length, which allows attackers to cause a denial of service (panic) via unspecified vectors, related to sctp_sf_violation_paramlen, sctp_sf_abort_violation, sctp_make_abort_violation, and incorrect data types in function calls.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00142945
9885	CVE-2008-4609	High		The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress.Please see also: http://blog.robertlee.name/2008/10/more-detailed-response-to-gordons-post.html and http://www.curbrisk.com/security-blog/robert-e-lee-discusses-tcp-denial-service-vulnerability-sc-magazine.html	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00186489
9886	CVE-2008-4576	High		sctp in Linux kernel before 2.6.25.18 allows remote attackers to cause a denial of service (OOPS) via an INIT-ACK that states the peer does not support AUTH, which causes the sctp_process_init function to clean up active transports and triggers the OOPS when the T1-Init timer expires.	Linux kernel before 2.6.25.18	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140677

	A	B	C	D	E	F	G	H	I	J	K	L	M
9887	CVE-2008-4554	Medium		The do_splice_from function in fs/splice.c in the Linux kernel before 2.6.27 does not reject file descriptors that have the O_APPEND flag set, which allows local users to bypass append mode and make arbitrary changes to other locations in the file.	Linux kernel before 2.6.27	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140702
9888	CVE-2008-4553	High		qemu-make-debian-root in qemu 0.9.1-5 on Debian GNU/Linux allows local users to overwrite arbitrary files via a symlink attack on temporary files and directories.	Qemu 0.9.1-5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140674
9889	CVE-2008-4552	High		nfs-utils 1.0.9, and possibly other versions before 1.1.3, invokes the host_ctl function with the wrong order of arguments, which causes TCP Wrappers to ignore netgroups and allows remote attackers to bypass intended access restrictions.	Patch from CVE-2008-1276 also fix this CVE	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131311
9890	CVE-2008-4539	High		Heap-based buffer overflow in the Cirrus VGA implementation in (1) KVM before kvm-82 and (2) QEMU on Debian GNU/Linux and Ubuntu might allow local users to gain privileges by using the VNC console for a connection, aka the LGD-54XX bitblt heap overflow. NOTE: this issue exists because of an incorrect fix for CVE-2007-1320.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00150967
9891	CVE-2008-4482	High		The XML parser in Xerces-C++ before 3.0.0 allows context-dependent attackers to cause a denial of service (stack consumption and crash) via an XML schema definition with a large maxOccurs value, which triggers excessive memory consumption during validation of an XML file.	Xerces-C++ before 3.0.0	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140746
9892	CVE-2008-4474	High		freeradius-dialupadmin in freeradius 2.0.4 allows local users to overwrite arbitrary files via a symlink attack on temporary files in (1) backup_radacct, (2) clean_radacct, (3) monthly_tot_stats, (4) tot_stats, and (5) truncate_radacct.	FreeRADIUS	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140712
9893	CVE-2008-4456	Low		Cross-site scripting (XSS) vulnerability in the command-line client in MySQL 5.0.26 through 5.0.45, when the --html option is enabled, allows attackers to inject arbitrary web script or HTML by placing it in a database cell, which might be accessed by this client when composing an HTML document.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140745
9894	CVE-2008-4445	Medium		The sctp_auth_ep_set_hmacs function in net/sctp/auth.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.26.4, when the SCTP-AUTH extension is enabled, does not verify that the identifier index is within the bounds established by SCTP_AUTH_HMAC_ID_MAX, which allows local users to obtain sensitive information via a crafted SCTP_HMAC_IDENT IOCTL request involving the sctp_getsockopt function, a different vulnerability than CVE-2008-4113.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140721
9895	CVE-2008-4410	Medium		The vmi_write_ldt_entry function in arch/x86/kernel/vmi_32.c in the Virtual Machine Interface (VMI) in the Linux kernel 2.6.26.5 invokes write_idt_entry where write_ldt_entry was intended, which allows local users to cause a denial of service (persistent application failure) via crafted function calls, related to the Java Runtime Environment (JRE) experiencing improper LDT selector state, a different vulnerability than CVE-2008-3247.	Linux kernel 2.6.26.5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140709
9896	CVE-2008-4409	Medium		libxml2 2.7.0 and 2.7.1 does not properly handle predefined entities definitions in entities, which allows context-dependent attackers to cause a denial of service (memory consumption and application crash), as demonstrated by use of xmllint on a certain XML document, a different vulnerability than CVE-2003-1564 and CVE-2008-3281.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140741
9897	CVE-2008-4395	High		Multiple buffer overflows in the ndiswrapper module 1.53 for the Linux kernel 2.6 allow remote attackers to execute arbitrary code by sending packets over a local wireless network that specify long ESSIDs.	ndiswrapper module is not shipped with wrlinux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144858
9898	CVE-2008-4316	Medium		Multiple integer overflows in glib/gbase64.c in GLib before 2.20 allow context-dependent attackers to execute arbitrary code via a long string that is converted either (1) from or (2) to a base64 representation.	glib	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00160586
9899	CVE-2008-4310	High		httputils.rb in WEBrick in Ruby 1.8.1 and 1.8.5 allows remote attackers to cause a denial of service (CPU consumption) via a crafted HTTP request. NOTE: this issue exists because of an incomplete fix for CVE-2008-3656.	ruby	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00149301
9900	CVE-2008-4309	Medium		The getbulk code in net-snmp 5.4 before 5.4.2.1, 5.3 before 5.3.2.3, and 5.2 before 5.2.5.1 allows remote attackers to cause a denial of service (crash) via vectors related to the number of responses or repeats.	net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00142934
9901	CVE-2008-4307	Medium		Race condition in the do_setlk function in fs/nfs/file.c in the Linux kernel before 2.6.26 allows local users to cause a denial of service (crash) via vectors resulting in an interrupted RPC call that leads to a stray FL_POSIX lock, related to improper handling of a race between fcntl and close in the EINTR case.	WRLinux doesn't ship linux kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00152431
9902	CVE-2008-4302	Medium		fs/splice.c in the splice subsystem in the Linux kernel before 2.6.22.2 does not properly handle a failure of the add_to_page_cache_lru function, and subsequently attempts to unlock a page that was not locked, which allows local users to cause a denial of service (kernel BUG and system crash), as demonstrated by the fio I/O tool.	Linux kernel before 2.6.22.2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138305
9903	CVE-2008-4226	High		Integer overflow in the xmlSAX2Characters function in libxml2 2.7.2 allows context-dependent attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a large XML document.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00146844
9904	CVE-2008-4225	High		Integer overflow in the xmlBufferResize function in libxml2 2.7.2 allows context-dependent attackers to cause a denial of service (infinite loop) via a large XML document.	libxml2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00146833

	A	B	C	D	E	F	G	H	I	J	K	L	M
9905	CVE-2008-4210	Medium		fs/open.c in the Linux kernel before 2.6.22 does not properly strip setuid and setgid bits when there is a write to a file, which allows local users to gain the privileges of a different group, and obtain sensitive information or possibly have unspecified other impact, by creating an executable file in a setgid directory through the (1) truncate or (2) ftruncate function in conjunction with memory-mapped I/O.	Linux kernel before 2.6.22.2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138329
9906	CVE-2008-4163	High		Unspecified vulnerability in ISC BIND 9.3.5-P2-W1, 9.4.2-P2-W1, and 9.5.0-P2-W1 on Windows allows remote attackers to cause a denial of service (UDP client handler termination) via unknown vectors.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138286
9907	CVE-2008-4113	Medium		The sctp_getsockopt_hmac_ident function in net/sctp/socket.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.26.4, when the SCTP-AUTH extension is enabled, relies on an untrusted length value to limit copying of data from kernel memory, which allows local users to obtain sensitive information via a crafted SCTP_HMAC_IDENT IOCTL request involving the sctp_getsockopt function.	Linux kernel before 2.6.26.4	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138320
9908	CVE-2008-4109	Medium		A certain Debian patch for OpenSSH before 4.3p2-9etch3 on etch, and before 4.6p1-1 on sid and lenny, uses functions that are not async-signal-safe in the signal handler for login timeouts, which allows remote attackers to cause a denial of service (connection slot exhaustion) via multiple login attempts. NOTE: this issue exists because of an incorrect fix for CVE-2006-5051.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138288
9909	CVE-2008-4108	High		Tools/faqwiz/move-faqwiz.sh (aka the generic FAQ wizard moving tool) in Python 2.4.5 might allow local users to overwrite arbitrary files via a symlink attack on a tmp$RANDOM.tmp temporary file. NOTE: there may not be common usage scenarios in which tmp$RANDOM.tmp is located in an untrusted directory.	Python 2.4.5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138274
9910	CVE-2008-4101	High		Vim 3.0 through 7.x before 7.2.010 does not properly escape characters, which allows user-assisted attackers to (1) execute arbitrary shell commands by entering a K keystroke on a line that contains a ; (semicolon) followed by a command, or execute arbitrary Ex commands by entering an argument after a (2) Ctrl-] (control close-square-bracket) or (3) g] (g close-square-bracket) keystroke sequence, a different issue than CVE-2008-2712.	Vim 3.0 through 7.x before 7.2.010	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138277
9911	CVE-2008-4098	Medium		MySQL before 5.0.67 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL home data directory. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4097.	MySQL before 5.0.67	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138291
9912	CVE-2008-4097	Medium		MySQL 5.0.51a allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are associated with symlinks within pathnames for subdirectories of the MySQL home data directory, which are followed when tables are created in the future. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-2079.	MySQL 5.0.51a	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138272
9913	CVE-2008-3970	Medium		pam_mount 0.10 through 0.45, when luserconf is enabled, does not verify mountpoint and source ownership before mounting a user-defined volume, which allows local users to bypass intended access restrictions via a local mount.	wrlinux doesn't support pam_mount, so we withdraw it.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135380
9914	CVE-2008-3964	Medium		Multiple off-by-one errors in libpng before 1.2.32beta01, and 1.4 before 1.4.0beta34, allow context-dependent attackers to cause a denial of service (crash) or have unspecified other impact via a PNG image with crafted zTXt chunks, related to (1) the png_push_read_zTXt function in pngread.c, and possibly related to (2) pngtest.c.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135361
9915	CVE-2008-3963	Medium		MySQL 5.0 before 5.0.66, 5.1 before 5.1.26, and 6.0 before 6.0.6 does not properly handle a b" (b single-quote single-quote) token, aka an empty bit-string literal, which allows remote attackers to cause a denial of service (daemon crash) by using this token in a SQL statement.	MySQL 5.0 before 5.0.66, 5.1 before 5.1.26, and 6.0 before 6.0.6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135334
9916	CVE-2008-3916	High		Heap-based buffer overflow in the strip_escapes function in signal.c in GNU ed before 1.0 allows context-dependent or user-assisted attackers to execute arbitrary code via a long filename. NOTE: since ed itself does not typically run with special privileges, this issue only crosses privilege boundaries when ed is invoked as a third-party component.http://xforce.iss.net/xforce/xfdb/44643 GNU ed is vulnerable to a heap-based buffer overflow, caused by improper bounds checking by the strip_escapes() function. By persuading a victim to open a specially-crafted file, a remote attacker could overflow a buffer and execute arbitrary code on the system.	GNU ed before 1.0	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135358
9917	CVE-2008-3915	High		Buffer overflow in nfsd in the Linux kernel before 2.6.26.4, when NFSv4 is enabled, allows remote attackers to have an unknown impact via vectors related to decoding an NFSv4 acl.	Linux kernel before 2.6.26.4	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135341
9918	CVE-2008-3911	High		The proc_do_xprt function in net/sunrpc/sysctl.c in the Linux kernel 2.6.26.3 does not check the length of a certain buffer obtained from userspace, which allows local users to overflow a stack-based buffer and have unspecified other impact via a crafted read system call for the /proc/sys/sunrpc/transports file.	Linux kernel 2.6.26.3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135329

	A	B	C	D	E	F	G	H	I	J	K	L	M
9919	CVE-2008-3896	Low		Grub Legacy 0.97 and earlier stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer before and after use, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.	Grub Legacy 0.97 and earlier	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135354
9920	CVE-2008-3844	High		Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as distributed in August 2008 by servers outside Red Hat but signed with a Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: the scope of this vulnerability is restricted to users who may have obtained packages through unofficial distribution points.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00133055
9921	CVE-2008-3833	Medium		The generic_file_splice_write function in fs/splice.c in the Linux kernel before 2.6.19 does not properly strip setuid and setgid bits when there is a write to a file, which allows local users to gain the privileges of a different group, and obtain sensitive information or possibly have unspecified other impact, by splicing into an inode in order to create an executable file in a setgid directory, a different vulnerability than CVE-2008-4210.	Linux kernel before 2.6.19	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140698
9922	CVE-2008-3832	Medium		A certain Fedora patch for the utrace subsystem in the Linux kernel before 2.6.26.5-28 on Fedora 8, and before 2.6.26.5-45 on Fedora 9, allows local users to cause a denial of service (NULL pointer dereference and system crash or hang) via a call to the utrace_control function.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140716
9923	CVE-2008-3831	Medium		The i915 driver in (1) drivers/char/drm/i915_dma.c in the Linux kernel 2.6.24 on Debian GNU/Linux and (2) sys/dev/pci/drm/i915_drv.c in OpenBSD does not restrict the DRM_I915_HWS_ADDR ioctl to the Direct Rendering Manager (DRM) master, which allows local users to cause a denial of service (memory corruption) via a crafted ioctl call, related to absence of the DRM_MASTER and DRM_ROOT_ONLY flags in the ioctl's configuration.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00142927
9924	CVE-2008-3825	Medium		pam_krb5 2.2.14 in Red Hat Enterprise Linux (RHEL) 5 and earlier, when the existing_ticket option is enabled, uses incorrect privileges when reading a Kerberos credential cache, which allows local users to gain privileges by setting the KRB5CCNAME environment variable to an arbitrary cache filename and running the (1) su or (2) sudo program. NOTE: there may be a related vector involving sshd that has limited relevance.	pam_krb5 2.2.14	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140675
9925	CVE-2008-3792	High		net/sctp/socket.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.26.4 does not verify that the SCTP-AUTH extension is enabled before proceeding with SCTP-AUTH API functions, which allows attackers to cause a denial of service (NULL pointer dereference and panic) via vectors that result in calls to (1) sctp_setsockopt_auth_chunk, (2) sctp_setsockopt_hmac_ident, (3) sctp_setsockopt_auth_key, (4) sctp_setsockopt_active_key, (5) sctp_setsockopt_del_key, (6) sctp_getsockopt_maxburst, (7) sctp_getsockopt_active_key, (8) sctp_getsockopt_peer_auth_chunks, or (9) sctp_getsockopt_local_auth_chunks.	Linux kernel before 2.6.26.4	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135365
9926	CVE-2008-3746	Medium		neon 0.28.0 through 0.28.2 allows remote servers to cause a denial of service (NULL pointer dereference and crash) via vectors related to Digest authentication and Digest domain parameter support.	neon	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00133067
9927	CVE-2008-3686	Medium		The rt6_fill_node function in Linux kernel 2.6.26-rc4, 2.6.26.2, and possibly other 2.6.26 versions, allows local users to cause a denial of service (kernel OOPS) via IPv6 requests when no IPv6 input device is in use, which triggers a NULL pointer dereference.	Linux Audit before 1.7	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131334
9928	CVE-2008-3652	High		src/racoon/handler.c in racoon in ipsec-tools does not remove an orphaned ph1 (phase 1) handle when it has been initiated remotely, which allows remote attackers to cause a denial of service (resource consumption).	IPsec-Tools racoon.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131305
9929	CVE-2008-3651	Medium		Memory leak in racoon/proposal.c in the racoon daemon in ipsec-tools before 0.7.1 allows remote authenticated users to cause a denial of service (memory consumption) via invalid proposals.	Linux ipsec_tools_racoon_daemon.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131290
9930	CVE-2008-3535	Medium		Off-by-one error in the iov_iter_advance function in mm/filemap.c in the Linux kernel before 2.6.27-rc2 allows local users to cause a denial of service (system crash) via a certain sequence of file I/O operations with readv and writev, as demonstrated by testcases/kernel/fs/ftest/ftest03 from the Linux Test Project.	Linux Audit before 1.7	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131344
9931	CVE-2008-3534	Medium		The shmem_delete_inode function in mm/shmem.c in the tmpfs implementation in the Linux kernel before 2.6.26.1 allows local users to cause a denial of service (system crash) via a certain sequence of file create, remove, and overwrite operations, as demonstrated by the insserv program, related to allocation of useless pages and improper maintenance of the i_blocks count.	Linux kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131293
9932	CVE-2008-3529	High		Heap-based buffer overflow in the xmlParseAttValueComplex function in parser.c in libxml2 before 2.7.0 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long XML entity name.	Libxml2 before 2.7.0	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135383

	A	B	C	D	E	F	G	H	I	J	K	L	M
9933	CVE-2008-3528	High		The error-reporting functionality in (1) fs/ext2/dir.c, (2) fs/ext3/dir.c, and possibly (3) fs/ext4/dir.c in the Linux kernel 2.6.26.5 does not limit the number of printk console messages that report directory corruption, which allows physically proximate attackers to cause a denial of service (temporary system hang) by mounting a filesystem that has corrupted dir->i_size and dir->i_blocks values and performing (a) read or (b) write operations. NOTE: there are limited scenarios in which this crosses privilege boundaries.	Linux kernel 2.6.26.5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138327
9934	CVE-2008-3527	Medium		arch/i386/kernel/sysenter.c in the Virtual Dynamic Shared Objects (vDSO) implementation in the Linux kernel before 2.6.21 does not properly check boundaries, which allows local users to gain privileges or cause a denial of service via unspecified vectors, related to the install_special_mapping, syscall, and syscall32_nopage functions.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00144890
9935	CVE-2008-3526	High		Integer overflow in the sctp_setsockopt_auth_key function in net/sctp/socket.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel 2.6.24-rc1 through 2.6.26.3 allows remote attackers to cause a denial of service (panic) or possibly have unspecified other impact via a crafted sca_keylength field associated with the SCTP_AUTH_KEY option.	Linux kernel 2.6.24-rc1 through 2.6.26.3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00133071
9936	CVE-2008-3525	High		The sbni_ioctl function in drivers/net/wan/sbni.c in the wan subsystem in the Linux kernel 2.6.26.3 does not check for the CAP_NET_ADMIN capability before processing a (1) SIOCDEVRESINSTATS, (2) SIOCDEVSHWSTATE, (3) SIOCDEVENSLAVE, or (4) SIOCDEVEMANSIPATE ioctl request, which allows local users to bypass intended capability restrictions.	Linux kernel 2.6.26.3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00135332
9937	CVE-2008-3524	Low		rc.sysinit in initscripts before 8.76.3-1 in Fedora 9 allows local users to delete arbitrary files via a symlink attack on a file or directory under (1) /var/lock or (2) /var/run.	initscripts	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00138293
9938	CVE-2008-3502	High		Unspecified vulnerability in Best Practical Solutions RT 3.0.0 through 3.6.6 allows remote authenticated users to cause a denial of service (CPU or memory consumption) via unspecified vectors related to the Devel::StackTrace module for Perl.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131318
9939	CVE-2008-3496	High		Buffer overflow in format descriptor parsing in the uvc_parse_format function in drivers/media/video/uvc/uvc_driver.c in uvcvideo in the video4linux (V4L) implementation in the Linux kernel before 2.6.26.1 has unknown impact and attack vectors.	Linux Audit before 1.7	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131342
9940	CVE-2008-3432	Medium		Heap-based buffer overflow in the mch_expand_wildcards function in os_unix.c in Vim 6.2 and 6.3 allows user-assisted attackers to execute arbitrary code via shell metacharacters in filenames, as demonstrated by the netrw.v3 test case.	Vim 6.2 and 6.3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00140676
9941	CVE-2008-3294	Medium		src/configure.in in Vim 5.0 through 7.1, when used for a build with Python support, does not ensure that the Makefile-conf temporary file has the intended ownership and permissions, which allows local users to execute arbitrary code by writing to this file during a time window associated with a race condition.	Vim 5.0 through 7.1	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00129884
9942	CVE-2008-3285	Medium		The Filesys::SmbClientParser module 2.7 and earlier for Perl allows remote SMB servers to execute arbitrary code via a folder name containing shell metacharacters.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00129886
9943	CVE-2008-3281	Medium		libxml2 2.6.32 and earlier does not properly detect recursion during entity expansion in an attribute value, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document.	Libxml2 2.6.32 and earlier	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00130238
9944	CVE-2008-3276	High		Integer overflow in the dccp_setsockopt_change function in net/dccp/proto.c in the Datagram Congestion Control Protocol (DCCP) subsystem in the Linux kernel 2.6.17-rc1 through 2.6.26.2 allows remote attackers to cause a denial of service (panic) via a crafted integer value, related to Change L and Change R options without at least one byte in the dccpsf_val field.	Linux Audit before 1.7	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00133054
9945	CVE-2008-3275	Medium		The (1) real_lookup and (2) __lookup_hash functions in fs/namei.c in the vfs implementation in the Linux kernel before 2.6.25.15 does not prevent creation of a child dentry for a deleted (aka S_DEAD) directory, which allows local users to cause a denial of service (overflow of the UBIFS orphan area) via a series of attempted file creations within deleted directories.	Linux kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131320
9946	CVE-2008-3272	Low		The snd_seq_oss_synth_make_info function in sound/core/seq/oss/seq_oss_synth.c in the sound subsystem in the Linux kernel before 2.6.27-rc2 does not verify that the device number is within the range defined by max_synthdev before returning certain data to the caller, which allows local users to obtain sensitive information.	Linux kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131300
9947	CVE-2008-3259	Low		OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some platforms to hijack the X11 forwarding port via a bind to a single IP address, as demonstrated on the HP-UX platform.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00129871
9948	CVE-2008-3247	High		The LDT implementation in the Linux kernel 2.6.25.x on x86_64 platforms uses an incorrect size for ldt_desc, which allows local users to cause a denial of service (system crash) or possibly gain privileges via unspecified vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00129861
9949	CVE-2008-3234	Medium		sshd in OpenSSH 4 on Debian GNU/Linux, and the 20070303 OpenSSH snapshot, allows remote authenticated users to obtain access to arbitrary SELinux roles by appending a :/ (colon slash) sequence, followed by the role name, to the username.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00129879

	A	B	C	D	E	F	G	H	I	J	K	L	M
9950	CVE-2008-3230	Low		The ffmpeg lavf demuxer allows user-assisted attackers to cause a denial of service (application crash) via a crafted GIF file, possibly related to gstreamer, as demonstrated by lol-giftopnm.gif.	ffmpeg	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00163951
9951	CVE-2008-3196	High		skeleton.c in yacc does not properly handle reduction of a rule with an empty right hand side, which allows context-dependent attackers to cause an out-of-bounds stack access when the yacc stack pointer points to the end of the stack.	skeleton.c in yacc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00129865
9952	CVE-2008-3144	Medium		Multiple integer overflows in the PyOS_vsnprintf function in Python/mysnprintf.c in Python 2.5.2 and earlier allow context-dependent attackers to cause a denial of service (memory corruption) or have unspecified other impact via crafted input to string formatting operations. NOTE: the handling of certain integer values is also affected by related integer underflows and an off-by-one error.	Python Software Foundation Python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131373
9953	CVE-2008-3143	High		Multiple integer overflows in Python before 2.5.2 might allow context-dependent attackers to have an unknown impact via vectors related to (1) Include/pymem.h; (2) _csv.c, (3) _struct.c, (4) arraymodule.c, (5) audioop.c, (6) binascii.c, (7) cPickle.c, (8) cStringIO.c, (9) cjkcodecs/multibytecodec.c, (10) datetimemodule.c, (11) md5.c, (12) rgbimgmodule.c, and (13) stropmodule.c in Modules/; (14) bufferobject.c, (15) listobject.c, and (16) obmalloc.c in Objects/; (17) Parser/node.c; and (18) asdl.c, (19) ast.c, (20) bltinmodule.c, and (21) compile.c in Python/, as addressed by checks for integer overflows, contributed by Google.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131389
9954	CVE-2008-3142	High		Multiple buffer overflows in Python 2.5.2 and earlier on 32bit platforms allow context-dependent attackers to cause a denial of service (crash) or have unspecified other impact via a long string that leads to incorrect memory allocation during Unicode string processing, related to the unicode_resize function and the PyMem_RESIZE macro.	Python Software Foundation Python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131371
9955	CVE-2008-3077	Medium		arch/x86/kernel/ptrace.c in the Linux kernel before 2.6.25.10 on the x86_64 platform leaks task_struct references into the sys32_ptrace function, which allows local users to cause a denial of service (system crash) or have unspecified other impact via unknown vectors, possibly a use-after-free vulnerability.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00128135
9956	CVE-2008-3076	High		The Netrw plugin 125 in netrw.vim in Vim 7.2a.10 allows user-assisted attackers to execute arbitrary code via shell metacharacters in filenames used by the execute and system functions within the (1) mz and (2) mc commands, as demonstrated by the netrw.v2 and netrw.v3 test cases. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2008-2712.	vim	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159140
9957	CVE-2008-3075	High		The shellescape function in Vim 7.0 through 7.2, including 7.2a.10, allows user-assisted attackers to execute arbitrary code via the ! (exclamation point) shell metacharacter in (1) the filename of a ZIP archive and possibly (2) the filename of the first file in a ZIP archive, which is not properly handled by zip.vim in the VIM ZIP plugin (zipPlugin.vim) v.11 through v.21, as demonstrated by the zipplugin and zipplugin.v2 test cases. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2008-2712. NOTE: this issue has the same root cause as CVE-2008-3074. NOTE: due to the complexity of the associated disclosures and the incomplete information related to them, there may be inaccuracies in this CVE description and in external mappings to this identifier.	vim	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158921
9958	CVE-2008-3074	High		The shellescape function in Vim 7.0 through 7.2, including 7.2a.10, allows user-assisted attackers to execute arbitrary code via the ! (exclamation point) shell metacharacter in (1) the filename of a tar archive and possibly (2) the filename of the first file in a tar archive, which is not properly handled by the VIM TAR plugin (tar.vim) v.10 through v.22, as demonstrated by the shellescape, tarplugin.v2, tarplugin, and tarplugin.Unchanged test cases. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2008-2712. NOTE: this issue has the same root cause as CVE-2008-3075. NOTE: due to the complexity of the associated disclosures and the incomplete information related to them, there may be inaccuracies in this CVE description and in external mappings to this identifier.	vim	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159068
9959	CVE-2008-2952	Medium		liblber/io.c in OpenLDAP 2.3.41, 2.3.42, and possibly other versions allows remote attackers to cause a denial of service (program termination) via crafted ASN.1 BER datagrams, which triggers an assertion error.	openldap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00128136
9960	CVE-2008-2944	Medium		Double free vulnerability in the utrace support in the Linux kernel, probably 2.6.18, in Red Hat Enterprise Linux (RHEL) 5 and Fedora Core 6 (FC6) allows local users to cause a denial of service (oops), as demonstrated by a crash when running the GNU GDB testsuite, a different vulnerability than CVE-2008-2365.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127081
9961	CVE-2008-2939	Medium		Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via wildcards in a pathname in an FTP URI.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131372
9962	CVE-2008-2931	Medium		The do_change_type function in fs/namespace.c in the Linux kernel before 2.6.22 does not verify that the caller has the CAP_SYS_ADMIN capability, which allows local users to gain privileges or cause a denial of service by modifying the properties of a mountpoint.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00128137

	A	B	C	D	E	F	G	H	I	J	K	L	M
9963	CVE-2008-2827	Medium		The rmtree function in lib/File/Path.pm in Perl 5.10 does not properly check permissions before performing a chmod, which allows local users to modify the permissions of arbitrary files via a symlink attack, a different vulnerability than CVE-2005-0448 and CVE-2004-0452.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127067
9964	CVE-2008-2826	Medium		Integer overflow in the sctp_getsockopt_local_addrs_old function in net/sctp/socket.c in the Stream Control Transmission Protocol (sctp) functionality in the Linux kernel before 2.6.25.9 allows local users to cause a denial of service (resource consumption and system outage) via vectors involving a large addr_num field in an sctp_getaddrs_old data structure.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00128134
9965	CVE-2008-2812	Medium		The Linux kernel before 2.6.25.10 does not properly perform tty operations, which allows local users to cause a denial of service (system crash) or possibly gain privileges via vectors involving NULL pointer dereference of function pointers in (1) hamradio/6pack.c, (2) hamradio/mkiss.c, (3) irda/irtty-sir.c, (4) ppp_async.c, (5) ppp_synctty.c, (6) slip.c, (7) wan/x25_asy.c, and (8) wireless/strip.c in drivers/net/.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00128132
9966	CVE-2008-2750	High		The pppol2tp_recvmsg function in drivers/net/pppol2tp.c in the Linux kernel 2.6 before 2.6.26-rc6 allows remote attackers to cause a denial of service (kernel heap memory corruption and system crash) and possibly have unspecified other impact via a crafted PPPOL2TP packet that results in a large value for a certain length variable.	Linux kernel 2.6 before 2.6.26-rc6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127062
9967	CVE-2008-2729	Medium		arch/x86_64/lib/copy_user.S in the Linux kernel before 2.6.19 on some AMD64 systems does not erase destination memory locations after an exception during kernel memory copy, which allows local users to obtain sensitive information.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127075
9968	CVE-2008-2712	High		Vim 7.1.314, 6.4, and other versions allows user-assisted remote attackers to execute arbitrary commands via Vim scripts that do not properly sanitize inputs before invoking the execute or system functions, as demonstrated using (1) filetype.vim, (2) zipplugin, (3) xpm.vim, (4) gzip_vim, and (5) netrw.	Vim 7.1.314, 6.4, and other versions	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127054
9969	CVE-2008-2384	High		SQL injection vulnerability in mod_auth_mysql.c in the mod-auth-mysql (aka libapache2-mod-auth-mysql) module for the Apache HTTP Server 2.x allows remote attackers to execute arbitrary SQL commands via multibyte character encodings for unspecified input.Please note that this describes the software used in debian as mod-auth-mysql (binary name is libapache2-mod-auth-mysql). It is different from the Sourceforge project.	Apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154973
9970	CVE-2008-2383	High		CRLF injection vulnerability in xterm allows user-assisted attackers to execute arbitrary commands via LF (aka \n) characters surrounding a command name within a Device Control Request Status String (DECRQSS) escape sequence in a text file, a related issue to CVE-2003-0063 and CVE-2003-0071.	Xterm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00152473
9971	CVE-2008-2382	Medium		The protocol_client_msg function in vnc.c in the VNC server in (1) Qemu 0.9.1 and earlier and (2) KVM kvm-79 and earlier allows remote attackers to cause a denial of service (infinite loop) via a certain message.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00150987
9972	CVE-2008-2375	High		Memory leak in a certain Red Hat deployment of vsftpd before 2.0.5 on Red Hat Enterprise Linux (RHEL) 3 and 4, when PAM is used, allows remote attackers to cause a denial of service (memory consumption) via a large number of invalid authentication attempts within the same session, a different vulnerability than CVE-2007-5962.	vsftpd before 2.0.5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127097
9973	CVE-2008-2372	Medium		The Linux kernel 2.6.24 and 2.6.25 before 2.6.25.9 allows local users to cause a denial of service (memory consumption) via a large number of calls to the get_user_pages function, which lacks a ZERO_PAGE optimization and results in allocation of useless Unchangedly zeroed pages.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00128130
9974	CVE-2008-2371	High		Heap-based buffer overflow in pcre_compile.c in the Perl-Compatible Regular Expression (PCRE) library 7.7 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a regular expression that begins with an option and contains multiple branches.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00126076
9975	CVE-2008-2365	Medium		Race condition in the ptrace and utrace support in the Linux kernel 2.6.9 through 2.6.25, as used in Red Hat Enterprise Linux (RHEL) 4, allows local users to cause a denial of service (oops) via a long series of PTRACE_ATTACH ptrace calls to another user's process that trigger a conflict between utrace_detach and report_quiescent, related to late ptrace_may_attach() check and race around &dead_engine_ops setting, a different vulnerability than CVE-2007-0771 and CVE-2008-1514.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127032
9976	CVE-2008-2358	High		The Datagram Congestion Control Protocol (DCCP) subsystem in the Linux kernel 2.6.18, and probably other versions, does not properly check feature lengths, which might allow remote attackers to execute arbitrary code, related to an unspecified overflow.	Linux kernel 2.6.18	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00125730
9977	CVE-2008-2327	High		Multiple buffer underflows in the (1) LZWDecode and (2) LZWDecodeCompat functions in tif_lzw.c in the LZW decoder in LibTIFF 3.8.2 and earlier allow context-dependent attackers to execute arbitrary code via a crafted TIFF file. NOTE: some of these details are obtained from third party information.	LibTIFF 3.8.2 and earlier	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00133061
9978	CVE-2008-2316	High		Integer overflow in _hashopenssl.c in the hashlib module in Python 2.5.2 and earlier might allow context-dependent attackers to defeat cryptographic digests, related to partial hashlib hashing of data exceeding 4GB.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131390

	A	B	C	D	E	F	G	H	I	J	K	L	M
9979	CVE-2008-2315	High		Multiple integer overflows in Python 2.5.2 and earlier allow context-dependent attackers to have an unknown impact via vectors related to the (1) stringobject, (2) unicodeobject, (3) bufferobject, (4) longobject, (5) tupleobject, (6) stropmodule, (7) gcmodule, and (8) mmapmodule modules.	python	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131356
9980	CVE-2008-2292	Medium		Buffer overflow in the __snprint_value function in snmp_get in Net-SNMP 5.1.4, 5.2.4, and 5.4.1, as used in SNMP.xs for Perl, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a large OCTETSTRING in an attribute value pair (AVP).	Net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00124764
9981	CVE-2008-2168	Medium		Cross-site scripting (XSS) vulnerability Apache 2.2.6 and earlier allows remote attackers to inject arbitrary web script or HTML via UTF-7 encoded URLs that are not properly handled when displaying the 403 Forbidden error page.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123765
9982	CVE-2008-2148	Low		The utimensat system call in Linux kernel 2.6.22 and other versions before 2.6.25.3 does not check file permissions when certain UTIME_NOW and UTIME_OMIT combinations are used, which allows local users to modify file times of arbitrary files, possibly leading to a denial of service.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123879
9983	CVE-2008-2137	Medium		The (1) sparc_mmap_check function in arch/sparc/kernel/sys_sparc.c and the (2) sparc64_mmap_check function in arch/sparc64/kernel/sys_sparc.c, in the Linux kernel before 2.6.25.3, omit some virtual-address range (aka span) checks when the mmap MAP_FIXED bit is not set, which allows local users to cause a denial of service (panic) via unspecified mmap calls.	WRlinux doesn't ship SPARC architecture.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00124772
9984	CVE-2008-2136	High		Memory leak in the ipip6_rcv function in net/ipv6/sit.c in the Linux kernel before 2.6.25.3 allows remote attackers to cause a denial of service (memory consumption) via network traffic to a Simple Internet Transition (SIT) tunnel interface, related to the pskb_may_pull and kfree_skb functions, and management of an skb reference count.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123369
9985	CVE-2008-2079	Medium		MySQL 4.1.x before 4.1.24, 5.0.x before 5.0.60, 5.1.x before 5.1.24, and 6.0.x before 6.0.5 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are within the MySQL home data directory, which can point to tables that are created in the future.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123874
9986	CVE-2008-2004	Medium		The drive_init function in QEMU 0.9.1 determines the format of a raw disk image based on the header, which allows local guest users to read arbitrary files on the host by modifying the header to identify a different format, which is used when the guest is restarted.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00124685
9987	CVE-2008-1946	Medium		The default configuration of su in /etc/pam.d/su in GNU coreutils 5.2.1 allows local users to gain the privileges of a (1) locked or (2) expired account by entering the account name on the command line, related to improper use of the pam_succeed_if.so module.	coreutils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00129860
9988	CVE-2008-1945	Medium		QEMU 0.9.0 does not properly handle changes to removable media, which allows guest OS users to read arbitrary files on the host OS by using the diskformat: parameter in the -usbdevice option to modify the disk-image header to identify a different format, a related issue to CVE-2008-2004.	QEMU.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131355
9989	CVE-2008-1927	Medium		Double free vulnerability in Perl 5.8.8 allows context-dependent attackers to cause a denial of service (memory corruption and crash) via a crafted regular expression containing UTF8 characters. NOTE: this issue might only be present on certain operating systems.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00122691
9990	CVE-2008-1887	High		Python 2.5.2 and earlier allows context-dependent attackers to execute arbitrary code via multiple vectors that cause a negative size value to provided to the PyString_FromStringAndSize function, which allocates less memory than expected when assert() is disabled and triggers a buffer overflow.	Python 2.5.2 and earlier	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00122602
9991	CVE-2008-1808	High		Multiple off-by-one errors in FreeType2 before 2.3.6 allow context-dependent attackers to execute arbitrary code via (1) a crafted table in a Printer Font Binary (PFB) file or (2) a crafted SHC instruction in a TrueType Font (TTF) file, which triggers a heap-based buffer overflow.	FreeType2 before 2.3.6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127050
9992	CVE-2008-1807	High		FreeType2 before 2.3.6 allow context-dependent attackers to execute arbitrary code via an invalid number of axes field in a Printer Font Binary (PFB) file, which triggers a free of arbitrary memory locations, leading to memory corruption.	FreeType2 before 2.3.6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127038
9993	CVE-2008-1721	High		Integer signedness error in the zlib extension module in Python 2.5.2 and earlier allows remote attackers to execute arbitrary code via a negative signed integer, which triggers insufficient memory allocation and a buffer overflow.	Python 2.5.2 and earlier	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00121223
9994	CVE-2008-1679	Medium		Multiple integer overflows in imageop.c in Python before 2.5.3 allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted images that trigger heap-based buffer overflows. NOTE: this issue is due to an incomplete fix for CVE-2007-4965.	Python before 2.5.3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00122686
9995	CVE-2008-1678	Medium		Memory leak in the zlib_stateful_init function in crypto/comp/c_zlib.c in libssl in OpenSSL 0.9.8f through 0.9.8h allows remote attackers to cause a denial of service (memory consumption) via multiple calls, as demonstrated by initial SSL client handshakes to the Apache HTTP Server mod_ssl that specify a compression algorithm.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00128128

	A	B	C	D	E	F	G	H	I	J	K	L	M
9996	CVE-2008-1675	High		The bdx_ioctl_priv function in the tehuti driver (tehuti.c) in Linux kernel 2.6.x before 2.6.25 does not properly check certain information related to register size, which has unspecified impact and local attack vectors, probably related to reading or writing kernel memory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123772
9997	CVE-2008-1673	High		The asn1 implementation in (a) the Linux kernel 2.4 before 2.4.36.6 and 2.6 before 2.6.25.5, as used in the cifs and ip_nat_snmp_basic modules; and (b) the gxsnmp package; does not properly validate length values during decoding of ASN.1 BER data, which allows remote attackers to cause a denial of service (crash) or execute arbitrary code via (1) a length greater than the working buffer, which can lead to an unspecified overflow; (2) an oid length of zero, which can lead to an off-by-one error; or (3) an indefinite length for a primitive encoding.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00125736
9998	CVE-2008-1672	Medium		OpenSSL 0.9.8f and 0.9.8g allows remote attackers to cause a denial of service (crash) via a TLS handshake that omits the Server Key Exchange message and uses particular cipher suites.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00125711
9999	CVE-2008-1669	Medium		Linux kernel before 2.6.25.2 does not apply a certain protection mechanism for fcntl functionality, which allows local users to (1) execute code in parallel or (2) exploit a race condition to obtain "re-ordered access to the descriptor table."	Linux kernel before 2.6.25.2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00122879
10000	CVE-2008-1657	Medium		OpenSSH before 4.9 allows remote authenticated users to bypass the sshd_config ForceCommand directive by modifying the .ssh/rc session file.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00121195
10001	CVE-2008-1628	Medium		Stack-based buffer overflow in the audit_log_user_command function in lib/audit_logging.c in Linux Audit before 1.7 might allow remote attackers to execute arbitrary code via a long command argument. NOTE: some of these details are obtained from third party information.	Linux Audit before 1.7	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00121211
10002	CVE-2008-1615	Medium		Linux kernel 2.6.18, and possibly other versions, when running on AMD64 architectures, allows local users to cause a denial of service (crash) via certain ptrace calls.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123753
10003	CVE-2008-1514	Medium		ptrace in Linux kernel 2.6.9 on Fedora 7 and 8 allows local users to cause a denial of service (kernel panic) via the user-area-padding test from the ptrace testsuite, which triggers an invalid dereference.	This is a Fedora specific problem	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00120113
10004	CVE-2008-1483	Medium		OpenSSH 4.3p2, and probably other versions, allows local users to hijack forwarded X connections by causing ssh to set DISPLAY to :10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs.	openssh 4.3p2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00120115
10005	CVE-2008-1447	High		The DNS protocol, as implemented in (1) BIND 8 and 9 before 9.5.0-P1, 9.4.2-P1, and 9.3.5-P1; (2) Microsoft DNS in Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2; and other implementations allow remote attackers to spoof DNS traffic via certain cache poisoning techniques against recursive resolvers, related to insufficient randomness of DNS transaction IDs and source ports, aka DNS Insufficient Socket Entropy Vulnerability.	bind	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00126632
10006	CVE-2008-1382	High		libpng 1.0.6 through 1.0.32, 1.2.0 through 1.2.26, and 1.4.0beta01 through 1.4.0beta19 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a PNG file with zero length "unknown" chunks, which trigger an access of uninitialized memory.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00121226
10007	CVE-2008-1376	High		A certain Red Hat build script for nfs-utils before 1.0.9-35z.el5_2 on Red Hat Enterprise Linux (RHEL) 5 omits TCP wrappers support, which might allow remote attackers to bypass intended access restrictions.	Nfs-utils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00131311
10008	CVE-2008-1375	Medium		Race condition in the directory notification subsystem (dnotify) in Linux kernel 2.6.x before 2.6.24.6, and 2.6.25 before 2.6.25.1, allows local users to cause a denial of service (OOPS) and possible gain privileges via unspecified vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00121877
10009	CVE-2008-1372	Medium		bzlib.c in bzip2 before 1.0.5 allows user-assisted remote attackers to cause a denial of service (crash) via a crafted file that triggers a buffer over-read, as demonstrated by the PROTOS GENOME test suite for Archive Formats.	bzip2 before 1.0.5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00120117
10010	CVE-2008-1367	High		gcc 4.3.x does not generate a cld instruction while compiling functions used for string manipulation such as memcpy and memmove on x86 and i386, which can prevent the direction flag (DF) from being reset in violation of ABI conventions and cause data to be copied in the wrong direction during signal handling in the Linux kernel, which might allow context-dependent attackers to trigger memory corruption. NOTE: this issue was originally reported for CPU consumption in SBCL.	WRLinux don't compile the kernel with gcc-4.3.x.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00120119
10011	CVE-2008-1294	Low		Linux kernel 2.6.17, and other versions before 2.6.22, does not check when a user attempts to set RLIMIT_CPU to 0 until after the change is made, which allows local users to bypass intended resource limits.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123777
10012	CVE-2008-0960	Medium		SNMPv3 HMAC verification in (1) Net-SNMP 5.2.x before 5.2.4.1, 5.3.x before 5.3.2.1, and 5.4.x before 5.4.1.1; (2) UCD-SNMP; (3) eCos; (4) Juniper Session and Resource Control (SRC) C-series 1.0.0 through 2.0.0; (5) NetApp (aka Network Appliance) Data ONTAP 7.3RC1 and 7.3RC2; (6) SNMP Research before 16.2; and (7) multiple Cisco IOS, CatOS, ACE, and Nexus products; relies on the client to specify the HMAC length, which makes it easier for remote attackers to bypass SNMP authentication via a length value of 1, which only checks the first byte.	Net-snmp	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00124113

	A	B	C	D	E	F	G	H	I	J	K	L	M
10013	CVE-2008-0948	High		Buffer overflow in the RPC library (lib/rpc/rpc_dtablesize.c) used by libgssrpc and kadmind in MIT Kerberos 5 (krb5) 1.2.2, and probably other versions before 1.3, when running on systems whose unistd.h does not define the FD_SETSIZE macro, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by triggering a large number of open file descriptors.	krb5 before 1.3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00120120
10014	CVE-2008-0947	High		Buffer overflow in the RPC library used by libgssrpc and kadmind in MIT Kerberos 5 (krb5) 1.4 through 1.6.3 allows remote attackers to execute arbitrary code by triggering a large number of open file descriptors.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00120120
10015	CVE-2008-0928	Medium		Qemu 0.9.1 and earlier does not perform range checks for block device read or write requests, which allows guest host users with root privileges to access arbitrary memory and escape the virtual machine.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156601
10016	CVE-2008-0891	Medium		Double free vulnerability in OpenSSL 0.9.8f and 0.9.8g, when the TLS server name extensions are enabled, allows remote attackers to cause a denial of service (crash) via a crafted packet. NOTE: some of these details are obtained from third party information.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00125706
10017	CVE-2008-0888	High		The NEEDBITS macro in the inflate_dynamic function in inflate.c for unzip can be invoked using invalid buffers, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors that trigger a free of uninitialized or previously-freed data.	There is no unzip package in WRLinux-1.4.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00120124
10018	CVE-2008-0731	High		The Linux kernel before 2.6.18.8-0.8 in SUSE openSUSE 10.2 does not properly handle failure of an AppArmor change_hat system call, which might allow attackers to trigger the unconfining of an apparmored task.	WRLinux didn't ship SUSE and openSUSE	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10460
10019	CVE-2008-0674	High		Buffer overflow in PCRE before 7.6 allows remote attackers to execute arbitrary code via a regular expression containing a character class with a large number of characters with Unicode code points greater than 255.	pcre before 7.6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118339
10020	CVE-2008-0600	High		The vmsplice_to_pipe function in Linux kernel 2.6.17 through 2.6.24.1 does not validate a certain userspace pointer before dereference, which allows local users to gain root privileges via crafted arguments in a vmsplice system call, a different vulnerability than CVE-2008-0009 and CVE-2008-0010.	Linux linux 2.6.17 through 2.6.24.1	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00117366
10021	CVE-2008-0598	Medium		Unspecified vulnerability in the 32-bit and 64-bit emulation in the Linux kernel 2.6.9, 2.6.18, and probably other versions allows local users to read uninitialized memory via unknown vectors involving a crafted binary.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00127030
10022	CVE-2008-0555	High		The ExpandCert function in Apache-SSL before apache_1.3.41+ssl_1.59 does not properly handle (1) '/' and (2) '=' characters in a Distinguished Name (DN) in a client certificate, which might allow remote attackers to bypass authentication via a crafted DN that triggers overwriting of environment variables.	Apache-SSL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00121215
10023	CVE-2008-0456	Low		CRLF injection vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary HTTP headers and conduct HTTP response splitting attacks by uploading a file with a multi-line name containing HTTP header sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118419
10024	CVE-2008-0455	Medium		Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.	apache 1.3.x before and include 1.3.39	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118418
10025	CVE-2008-0352	High		The Linux kernel 2.6.20 through 2.6.21.1 allows remote attackers to cause a denial of service (panic) via a certain IPv6 packet, possibly involving the Jumbo Payload hop-by-hop option (jumbogram).	linux kernel from 2.6.20 to 2.6.21.1	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00117211
10026	CVE-2008-0172	Medium		The get_repeat_type function in basic_regex_creator.hpp in the Boost regex library (aka Boost.Regex) in Boost 1.33 and 1.34 allows context-dependent attackers to cause a denial of service (NULL dereference and crash) via an invalid regular expression.	Boost 1.33 and 1.34	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118417
10027	CVE-2008-0171	Medium		regex/v4/perl_matcher_non_recursive.hpp in the Boost regex library (aka Boost.Regex) in Boost 1.33 and 1.34 allows context-dependent attackers to cause a denial of service (failed assertion and crash) via an invalid regular expression.	Boost 1.33 and 1.34	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118417
10028	CVE-2008-0163	Medium		Linux kernel 2.6, when using vservers, allows local users to access resources of other vservers via a symlink attack in /proc.	Linux kernel 2.6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156633
10029	CVE-2008-0063	Medium		The Kerberos 4 support in KDC in MIT Kerberos 5 (krb5kdc) does not properly clear the unused portion of a buffer when generating an error message, which might allow remote attackers to obtain sensitive information, aka "Uninitialized stack values."	krb5 vulnerability	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00120125
10030	CVE-2008-0062	High		KDC in MIT Kerberos 5 (krb5kdc) does not set a global variable for some krb4 message types, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted messages that trigger a NULL pointer dereference or double-free.	krb5 vulnerability	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00120131

	A	B	C	D	E	F	G	H	I	J	K	L	M
10031	CVE-2008-0010	Low		The copy_from_user_mmap_sem function in fs/splice.c in the Linux kernel 2.6.22 through 2.6.24 does not validate a certain userspace pointer before dereference, which allow local users to read from arbitrary kernel memory locations.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00117373
10032	CVE-2008-0007	High		Linux kernel before 2.6.22.17, when using certain drivers that register a fault handler that does not perform range checks, allows local users to access kernel memory via an out-of-range offset.	linux kernel before 2.6.22.17	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00117209
10033	CVE-2008-0005	Medium		mod_proxy_ftp in Apache 2.2.x before 2.2.7-dev, 2.0.x before 2.0.62-dev, and 1.3.x before 1.3.40-dev does not define a charset, which allows remote attackers to conduct cross-site scripting (XSS) attacks using UTF-7 encoding.	apache 1.3.x before 1.3.40	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118414
10034	CVE-2007-6762	High	CRITICAL	In the Linux kernel before 2.6.20, there is an off-by-one bug in net/netlabel/netlabel_cipso_v4.c where it is possible to overflow the doi_def->tags[] array.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-4552
10035	CVE-2007-6761			drivers/media/video/videobuf-vmalloc.c in the Linux kernel before 2.6.24 does not initialize videobuf_mapping data structures, which allows local users to trigger an incorrect count value and videobuf leak via unspecified vectors, a different vulnerability than CVE-2010-5321.	linux	Unchanged	Not vulnerable	Not vulnerable	Won't Fix	Won't Fix	Won't Fix	Won't Fix	LIN9-4027
10036	CVE-2007-6754	Medium		The ipalloc function in libc/stdlib/malloc.c in jemalloc in libc for FreeBSD 6.4 and NetBSD does not properly allocate memory, which makes it easier for context-dependent attackers to perform memory-related attacks such as buffer overflows via a large size value, related to integer rounding and overflow errors.	libc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366819
10037	CVE-2007-6750	Medium		The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.	apache http_server.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00328005
10038	CVE-2007-6733	Medium		The nfs_lock function in fs/nfs/file.c in the Linux kernel 2.6.9 does not properly remove POSIX locks on files that are setgid without group-execute permission, which allows local users to cause a denial of service (BUG and system crash) by locking a file on an NFS filesystem and then changing this file's permissions, a related issue to CVE-2010-0727.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00206483
10039	CVE-2007-6716	Medium		fs/direct-io.c in the dio subcystem in the Linux kernel before 2.6.23 does not properly zero out the dio struct, which allows local users to cause a denial of service (OOPS), as demonstrated by a certain fio test.	Linux kernel before 2.6.23	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154904
10040	CVE-2007-6712	Medium		Integer overflow in the hrtimer_forward function (hrtimer.c) in Linux kernel 2.6.21-rc4, when running on 64-bit systems, allows local users to cause a denial of service (infinite loop) via a timer with a large expiry value, which causes the timer to always be expired.	Linux kernel 2.6.21-rc4	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00154941
10041	CVE-2007-6698	Medium		The BDB backend for slapd in OpenLDAP before 2.3.36, allows remote authenticated users to cause a denial of service (crash) via a potentially-successful modify operation with the NOOP control set to critical, possibly due to a double free vulnerability.	openldap before 2.3.36	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118413
10042	CVE-2007-6514	Medium		Apache HTTP Server, when running on Linux with a document root on a Windows share mounted using smbfs, allows remote attackers to obtain unprocessed content such as source files for .php programs via a trailing "\ " (backslash), which is not handled by the intended AddType directive.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118352
10043	CVE-2007-6417	High		The shmem_getpage function (mm/shmem.c) in Linux kernel 2.6.11 through 2.6.23 does not properly clear allocated memory in some rare circumstances, which might allow local users to read sensitive kernel data or cause a denial of service (crash).	linux kernel from 2.6.11 to 2.6.23	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00114278
10044	CVE-2007-6388	Medium		Cross-site scripting (XSS) vulnerability in mod_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118351
10045	CVE-2007-6313	High		MySQL Server 5.1.x before 5.1.23 and 6.0.x before 6.0.4 does not check the rights of the entity executing BINLOG, which allows remote authorized users to execute arbitrary BINLOG statements.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156664
10046	CVE-2007-6304	Medium		The federated engine in MySQL 5.0.x before 5.0.52, 5.1.x before 5.1.23, and 6.0.x before 6.0.4, when performing a certain SHOW TABLE STATUS query, does not properly handle a response with a small number of columns, which allows remote MySQL servers to cause a denial of service (federated handler crash and daemon crash) via a response that lacks the minimum required number of columns.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00122976
10047	CVE-2007-6303	Low		MySQL 5.0.x before 5.0.52, 5.1.x before 5.1.23, and 6.0.x before 6.0.4 does not update the DEFINER value of a view when the view is altered, which allows remote authenticated users to gain privileges via a sequence of statements including a CREATE SQL SECURITY DEFINER VIEW statement and an ALTER VIEW statement.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00122976
10048	CVE-2007-6282	High		The IPsec implementation in Linux kernel before 2.6.25 allows remote routers to cause a denial of service (crash) via a fragmented ESP packet in which the first fragment does not contain the entire ESP header and IV.	Linux kernel before 2.6.25	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156675
10049	CVE-2007-6258	High		Multiple stack-based buffer overflows in the legacy mod_jk2 2.0.3-DEV and earlier Apache module allow remote attackers to execute arbitrary code via a long (1) Host header, or (2) Hostname within a Host header.	mod_jk2 2.0.3-DEV and earlier Apache module	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156696

	A	B	C	D	E	F	G	H	I	J	K	L	M
10050	CVE-2007-6206	Low		The do_coredump function in fs/exec.c in Linux kernel 2.4.x and 2.6.x up to 2.6.24-rc3, and possibly other versions, does not change the UID of a core dump file if it exists before a root process creates a core dump in the same location, which might allow local users to obtain sensitive information.	linux kernel 2.4.x and 2.6.x, up to 2.6.24-rc3	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00114305
10051	CVE-2007-6203	Medium		Apache HTTP Server 2.0.x and 2.2.x does not sanitize the HTTP Method specifier header from an HTTP request when it is reflected back in a "413 Request Entity Too Large" error message, which might allow cross-site scripting (XSS) style attacks using web client components that can send arbitrary headers in requests, as demonstrated via an HTTP request containing an invalid Content-length value, a similar issue to CVE-2006-3918.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118350
10052	CVE-2007-6200	High		Unspecified vulnerability in rsync before 3.0.0pre6, when running a writable rsync daemon, allows remote attackers to bypass exclude, exclude_from, and filter and read or write hidden files via (1) symlink, (2) partial-dir, (3) backup-dir, and unspecified (4) dest options.	rsync before 3.0.0pre6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118347
10053	CVE-2007-6199	High		rsync before 3.0.0pre6, when running a writable rsync daemon that is not using chroot, allows remote attackers to access restricted files via unknown vectors that cause rsync to create a symlink that points outside of the module's hierarchy.	rsync before 3.0.0pre6	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118347
10054	CVE-2007-6151	High		The isdn_ioctl function in isdn_common.c in Linux kernel 2.6.23 allows local users to cause a denial of service via a crafted ioctl struct in which iocts is not null terminated, which triggers a buffer overflow.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159243
10055	CVE-2007-6067	Medium		Algorithmic complexity vulnerability in the regular expression parser in TCL before 8.4.17, as used in PostgreSQL 8.2 before 8.2.6, 8.1 before 8.1.11, 8.0 before 8.0.15, and 7.4 before 7.4.19, allows remote authenticated users to cause a denial of service (memory consumption) via a crafted complex regular expression with doubly-nested states.	PostgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156621
10056	CVE-2007-6063	Medium		Buffer overflow in the isdn_net_setcfg function in isdn_net.c in Linux kernel 2.6.23 allows local users to have an unknown impact via a crafted argument to the isdn_ioctl function.	Linux kernel 2.6.23	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00113569
10057	CVE-2007-5972	High		Double free vulnerability in the krb5_def_store_mkey function in lib/kdb/kdb_default.c in MIT Kerberos 5 (krb5) 1.5 has unknown impact and remote authenticated attack vectors. NOTE: the free operations occur in code that stores the krb5kdc master key, and so the attacker must have privileges to store this key.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158923
10058	CVE-2007-5971	Medium		Double free vulnerability in the gss_krb5int_make_seal_token_v3 function in lib/gssapi/krb5/k5sealv3.c in MIT Kerberos 5 (krb5) has unknown impact and attack vectors.Information from Apple: http://docs.info.apple.com/article.html?artnum=307562	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159069
10059	CVE-2007-5970	Medium		MySQL 5.1.x before 5.1.23 and 6.0.x before 6.0.4 allows remote authenticated users to gain privileges on arbitrary tables via unspecified vectors involving use of table-level DATA DIRECTORY and INDEX DIRECTORY options when creating a partitioned table with the same name as a table on which the user lacks privileges.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158918
10060	CVE-2007-5969	Low		MySQL Community Server 5.0.x before 5.0.51, Enterprise Server 5.0.x before 5.0.52, Server 5.1.x before 5.1.23, and Server 6.0.x before 6.0.4, when a table relies on symlinks created through explicit DATA DIRECTORY and INDEX DIRECTORY options, allows remote authenticated users to overwrite system table information and gain privileges via a RENAME TABLE statement that changes the symlink to point to an existing file.	mysql	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159147
10061	CVE-2007-5966	High		Integer overflow in the hrtimer_start function in kernel/hrtimer.c in the Linux kernel before 2.6.23.10 allows local users to execute arbitrary code or cause a denial of service (panic) via a large relative timeout value. NOTE: some of these details are obtained from third party information.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159148
10062	CVE-2007-5962	High		Memory leak in a certain Red Hat patch, applied to vsftpd 2.0.5 on Red Hat Enterprise Linux (RHEL) 5 and Fedora 6 through 8, and on Foresight Linux and rPath appliances, allows remote attackers to cause a denial of service (memory consumption) via a large number of CWD commands, as demonstrated by an attack on a daemon with the deny_file configuration option.	Vsftpd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156659
10063	CVE-2007-5925	Medium		The convert_search_mode_to_innobase function in ha_innodb.cc in the InnoDB engine in MySQL 5.1.23-BK and earlier allows remote authenticated users to cause a denial of service (database crash) via a certain CONTAINS operation on an indexed column, which triggers an assertion error.	MySQL 5.1.23	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00113453
10064	CVE-2007-5908	High		Buffer overflow in the (1) sysfs_show_available_clocksources and (2) sysfs_show_current_clocksources functions in Linux kernel 2.6.23 and earlier might allow local users to cause a denial of service or execute arbitrary code via crafted clock source names.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10077
10065	CVE-2007-5904	High		Multiple buffer overflows in CIFS VFS in Linux kernel 2.6.23 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via long SMB responses that trigger the overflows in the SendReceive function.	Linux kernel 2.6.23	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00115027
10066	CVE-2007-5902	High		Integer overflow in the svcauth_gss_get_principal function in lib/rpc/svc_auth_gss.c in MIT Kerberos 5 (krb5) allows remote attackers to have an unknown impact via a large length value for a GSS client name in an RPC request.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159146

	A	B	C	D	E	F	G	H	I	J	K	L	M
10067	CVE-2007-5901	Medium		Use-after-free vulnerability in the gss_indicate_mechs function in lib/gssapi/mechglue/g_initialize.c in MIT Kerberos 5 (krb5) has unknown impact and attack vectors. NOTE: this might be the result of a typo in the source code.Information from Apple: http://docs.info.apple.com/article.html?artnum=307562	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159236
10068	CVE-2007-5894	High		** DISPUTED ** The reply function in ftpd.c in the gssftp ftpd in MIT Kerberos 5 (krb5) does not initialize the length variable when auth_type has a certain value, which has unknown impact and remote authenticated attack vectors. NOTE: the original disclosure misidentifies the conditions under which the uninitialized variable is used. NOTE: the vendor disputes this issue, stating 'The 'length' variable is only uninitialized if 'auth_type' is neither the 'KERBEROS_V4' nor 'GSSAPI'; this condition cannot occur in the unmodified source code.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159234
10069	CVE-2007-5846	High		The SNMP agent in net-snmp 5.4.1 and earlier allows remote attackers to cause a denial of service (CPU and memory consumption) via a GETBULK request with a large max-repeaters value.	This vulnerability affects net-snmp 5.4.1 and earlier ones.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00133922
10070	CVE-2007-5794	Medium		Race condition in nss_ldap, when used in applications that use pthread and fork after a call to nss_ldap, does not properly handle the LDAP connection, which might cause nss_ldap to return the wrong user data to the wrong process. NOTE: this issue was originally reported for Dovecot with the wrong mailboxes being returned, but other applications might also be affected.	Wrlinux doesn't ship nss_ldap.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118344
10071	CVE-2007-5708	High		slapo-pcache (overlays/pcache.c) in slapd in OpenLDAP before 2.3.39, when running as a proxy-caching server, allocates memory using a malloc variant instead of calloc, which prevents an array from being initialized properly and might allow attackers to cause a denial of service (segmentation fault) via unknown vectors that prevent the array from being null terminated.	openldap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00121798
10072	CVE-2007-5707	High		OpenLDAP before 2.3.39 allows remote attackers to cause a denial of service (slapd crash) via an LDAP request with a malformed objectClasses attribute. NOTE: this has been reported as a double free, but the reports are inconsistent.	openldap	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00121798
10073	CVE-2007-5503	High		Multiple integer overflows in Cairo before 1.4.12 might allow remote attackers to execute arbitrary code, as demonstrated using a crafted PNG image, which is not properly handled by the read_png function.	Cairo 1.4.12	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118346
10074	CVE-2007-5502	Medium		The PRNG implementation for the OpenSSL FIPS Object Module 1.1.1 does not perform auto-seeding during the FIPS self-test, which generates random data that is more predictable than expected and makes it easier for attackers to bypass protection mechanisms that rely on the randomness.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159239
10075	CVE-2007-5501	Medium		The tcp_sacktag_write_queue function in net/ipv4/tcp_input.c in Linux kernel 2.6.24-rc2 and earlier allows remote attackers to cause a denial of service (crash) via crafted ACK responses that trigger a NULL pointer dereference.	Linux kernel 2.6.24-rc2	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00122971
10076	CVE-2007-5500	Medium		The wait_task_stopped function in the Linux kernel before 2.6.23.8 checks a TASK_TRACED bit instead of an exit_state value, which allows local users to cause a denial of service (machine crash) via unspecified vectors. NOTE: some of these details are obtained from third party information.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158998
10077	CVE-2007-5498	Medium		The Xen hypervisor block backend driver for Linux kernel 2.6.18, when running on a 64-bit host with a 32-bit paravirtualized guest, allows local privileged users in the guest OS to cause a denial of service (host OS crash) via a request that specifies a large number of blocks.	Linux kernel 2.6.18	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156602
10078	CVE-2007-5497	Medium		Multiple integer overflows in libext2fs in e2fsprogs before 1.40.3 allow user-assisted remote attackers to execute arbitrary code via a crafted filesystem image.	e2fsprogs	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159144
10079	CVE-2007-5496	Low		Cross-site scripting (XSS) vulnerability in setroubleshoot 2.0.5 allows local users to inject arbitrary web script or HTML via a crafted (1) file or (2) process name, which triggers an Access Vector Cache (AVC) log entry in a log file used during composition of HTML documents for sealert.	setroubleshoot	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156706
10080	CVE-2007-5495	Medium		sealert in setroubleshoot 2.0.5 allows local users to overwrite arbitrary files via a symlink attack on the sealert.log temporary file.	WRLinux doesn't ship setroubleshoot.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156702
10081	CVE-2007-5269	High		Certain chunk handlers in libpng before 1.0.29 and 1.2.x before 1.2.21 allow remote attackers to cause a denial of service (crash) via crafted (1) pCAL (png_handle_pCAL), (2) sCAL (png_handle_sCAL), (3) tEXt (png_push_read_tEXt), (4) iTXt (png_handle_iTXt), and (5) ztXT (png_handle_ztXt) chunking in PNG images, which trigger out-of-bounds read operations.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00109671
10082	CVE-2007-5268	Medium		pngrtran.c in libpng before 1.0.29 and 1.2.x before 1.2.21 use (1) logical instead of bitwise operations and (2) incorrect comparisons, which might allow remote attackers to cause a denial of service (crash) via a crafted PNG image.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00109667
10083	CVE-2007-5267	Medium		Off-by-one error in ICC profile chunk handling in the png_set_iCCP function in pngset.c in libpng before 1.2.22 beta1 allows remote attackers to cause a denial of service (crash) via a crafted PNG image, due to an incorrect fix for CVE-2007-5266.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123887
10084	CVE-2007-5266	Medium		Off-by-one error in ICC profile chunk handling in the png_set_iCCP function in pngset.c in libpng before 1.0.29 beta1 and 1.2.x before 1.2.21 beta1 allows remote attackers to cause a denial of service (crash) via a crafted PNG image that prevents a name field from being NULL terminated.	libpng	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123887

	A	B	C	D	E	F	G	H	I	J	K	L	M
10085	CVE-2007-5199	High	Critical	A single byte overflow in catalogue.c in X.Org libXfont 1.3.1 allows remote attackers to have unspecified impact.	libxfont	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5152
10086	CVE-2007-5191	Medium		mount and umount in util-linux and loop-aes-utils call the setuid and setgid functions in the wrong order and do not check the return values, which might allow attackers to gain privileges via helpers such as mount.nfs.	Investigating possible vulnerability in the Linux kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	9196
10087	CVE-2007-5135	Medium		Off-by-one error in the SSL_get_shared_ciphers function in OpenSSL 0.9.7 up to 0.9.7l, and 0.9.8 up to 0.9.8f, might allow remote attackers to execute arbitrary code via a crafted packet that triggers a one-byte buffer underflow. NOTE: this issue was introduced as a result of a fix for CVE-2006-3738. As of 20071012, it is unknown whether code execution is possible.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	9194
10088	CVE-2007-5116	High		Buffer overflow in the polymorphic opcode support in the Regular Expression Engine (regcomp.c) in Perl 5.8 allows context-dependent attackers to execute arbitrary code by switching from byte to Unicode (UTF) characters in a regular expression.	Perl 5.8	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118333
10089	CVE-2007-5001	Medium		Linux kernel before 2.4.21 allows local users to cause a denial of service (kernel panic) via asynchronous input or output on a FIFO special file.	Linux kernel before 2.4.21	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156686
10090	CVE-2007-5000	Medium		Cross-site scripting (XSS) vulnerability in the (1) mod_imap module in the Apache HTTP Server 1.3.0 through 1.3.39 and 2.0.35 through 2.0.61 and the (2) mod_imagemap module in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159071
10091	CVE-2007-4998	Medium		cp, when running with an option to preserve symlinks on multiple OSes, allows local, user-assisted attackers to overwrite arbitrary files via a symlink attack using crafted directories containing multiple source files that are copied to the same destination.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156669
10092	CVE-2007-4997	Medium		Integer underflow in the ieee80211_rx function in net/ieee80211/ieee80211_rx.c in the Linux kernel 2.6.x before 2.6.23 allows remote attackers to cause a denial of service (crash) via a crafted SKB length value in a runt IEEE 802.11 frame when the IEEE80211_STYPE_QOS_DATA flag is set, aka an "off-by-two error."	Linux kernel 2.6.23	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00113164
10093	CVE-2007-4995	High		Off-by-one error in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8f allows remote attackers to execute arbitrary code via unspecified vectors.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00125713
10094	CVE-2007-4965	Medium		Multiple integer overflows in the imageop module in Python 2.5.1 and earlier allow context-dependent attackers to cause a denial of service (application crash) and possibly obtain sensitive information (memory contents) via crafted arguments to (1) the tovideo method, and unspecified other vectors related to (2) imageop.c, (3) rbgimgmodule.c, and other files, which trigger heap-based buffer overflows.	python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268347
10095	CVE-2007-4849	Medium		JFFS2, as used on One Laptop Per Child (OLPC) build 542 and possibly other Linux systems, when POSIX ACL support is enabled, does not properly store permissions during (1) inode creation or (2) ACL setting, which might allow local users to access restricted files or directories after a remount of a filesystem, related to legacy modes and an inconsistency between dentry permissions and inode permissions.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00115560
10096	CVE-2007-4829	Medium		Directory traversal vulnerability in the Archive::Tar Perl module 1.36 and earlier allows user-assisted remote attackers to overwrite arbitrary files via a TAR archive that contains a file whose name is an absolute path or has ".." sequences.	WRLinux didn't ship package perl-Archive-Tar.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	10064
10097	CVE-2007-4772	Medium		The regular expression parser in TCL before 8.4.17, as used in PostgreSQL 8.2 before 8.2.6, 8.1 before 8.1.11, 8.0 before 8.0.15, and 7.4 before 7.4.19, allows context-dependent attackers to cause a denial of service (infinite loop) via a crafted regular expression.	PostgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156712
10098	CVE-2007-4769	Medium		The regular expression parser in TCL before 8.4.17, as used in PostgreSQL 8.2 before 8.2.6, 8.1 before 8.1.11, 8.0 before 8.0.15, and 7.4 before 7.4.19, allows remote authenticated users to cause a denial of service (backend crash) via an out-of-bounds backref number.	PostgreSQL	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156630
10099	CVE-2007-4768	High		Heap-based buffer overflow in Perl-Compatible Regular Expression (PCRE) library before 7.3 allows context-dependent attackers to execute arbitrary code via a singleton Unicode sequence in a character class in a regex pattern, which is incorrectly optimized.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118339
10100	CVE-2007-4767	Medium		Perl-Compatible Regular Expression (PCRE) library before 7.3 does not properly compute the length of (1) a \p sequence, (2) a \P sequence, or (3) a \ P{x} sequence, which allows context-dependent attackers to cause a denial of service (infinite loop or crash) or execute arbitrary code.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118335
10101	CVE-2007-4766	High		Multiple integer overflows in Perl-Compatible Regular Expression (PCRE) library before 7.3 allow context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via unspecified escape (backslash) sequences.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118339
10102	CVE-2007-4752	High		ssh in OpenSSH before 4.7 does not properly handle when an untrusted cookie cannot be created and uses a trusted X11 cookie instead, which allows attackers to violate intended policy and gain privileges by causing an X client to be treated as trusted.	openssh.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231173
10103	CVE-2007-4567	High		Linux kernel 2.6.22 and earlier, and possibly other versions, does not properly validate the hop-by-hop IPv6 extended header, which allows remote attackers to cause a denial of service (kernel panic) via a crafted IPv6 packet.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158919

	A	B	C	D	E	F	G	H	I	J	K	L	M
10104	CVE-2007-4559	Medium		Directory traversal vulnerability in the (1) extract and (2) extractall functions in the tarfile module in Python allows user-assisted remote attackers to overwrite arbitrary files via a .. (dot dot) sequence in filenames in a TAR archive, a related issue to CVE-2001-1267.	python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268329
10105	CVE-2007-4476	High		Buffer overflow in the safer_name_suffix function in GNU tar has unspecified attack vectors and impact, resulting in a crashing stack.	tar	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00115672
10106	CVE-2007-4133	Medium		The (1) hugetlb_vmtruncate_list and (2) hugetlb_vmtruncate functions in fs/hugetlbfs/inode.c in the Linux kernel before 2.6.19-rc4 perform certain prio_tree calculations using HPAGE_SIZE instead of PAGE_SIZE units, which allows local users to cause a denial of service (panic) via unspecified vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00110680
10107	CVE-2007-4130	High		The Linux kernel 2.6.9 before 2.6.9-67 in Red Hat Enterprise Linux (RHEL) 4 on Itanium (ia64) does not properly handle page faults during NUMA memory access, which allows local users to cause a denial of service (panic) via invalid arguments to set_mempolicy in an MPOL_BIND operation.	The Linux kernel 2.6.9 before 2.6.9-67	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156642
10108	CVE-2007-3999	High		Stack-based buffer overflow in the svcauth_gss_validate function in lib/rpc/svc_auth_gss.c in the RPCSEC_GSS RPC library (librpcsecgss) in MIT Kerberos 5 (krb5) 1.4 through 1.6.2, as used by the Kerberos administration daemon (kadmind) and some third-party applications that use krb5, allows remote attackers to cause a denial of service (daemon crash) and probably execute arbitrary code via a long string in an RPC message.	krb5.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00267986
10109	CVE-2007-3850	Low		The eHCA driver in Linux kernel 2.6 before 2.6.22, when running on PowerPC, does not properly map userspace resources, which allows local users to read portions of physical address space.	Investigating possible vulnerability in the Linux kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00123893
10110	CVE-2007-3849	Low		Red Hat Enterprise Linux (RHEL) 5 ships the rpm for the Advanced Intrusion Detection Environment (AIDE) before 0.13.1 with a database that lacks checksum information, which allows context-dependent attackers to bypass file integrity checks and modify certain files.	rpm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00112683
10111	CVE-2007-3798	Medium		Integer overflow in print-bgp.c in the BGP dissector in tcpdump 3.9.6 and earlier allows remote attackers to execute arbitrary code via crafted TLVs in a BGP packet, related to an unchecked return value.	tcpdump	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268348
10112	CVE-2007-3731	Medium		The Linux kernel 2.6.20 and 2.6.21 does not properly handle an invalid LDT segment selector in %cs (the xcs field) during ptrace single-step operations, which allows local users to cause a denial of service (NULL dereference and OOPS) via certain code that makes ptrace PTRACE_SETREGS and PTRACE_SINGLESTEP requests, related to the TRACE_IRQS_ON function, and possibly related to the arch_ptrace function.	linux linux_kernel.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268323
10113	CVE-2007-3108	Low		The BN_from_montgomery function in crypto/bn/bn_mont.c in OpenSSL 0.9.8e and earlier does not properly perform Montgomery multiplication, which might allow local users to conduct a side-channel attack and retrieve RSA private keys.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268006
10114	CVE-2007-3102	Medium		Unspecified vulnerability in the linux_audit_record_event function in OpenSSH 4.3p2, as used on Fedora Core 6 and possibly other systems, allows remote attackers to write arbitrary characters to an audit log via a crafted username. NOTE: some of these details are obtained from third party information.	openssh	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	9202
10115	CVE-2007-2953	Medium		Format string vulnerability in the helptags_one function in src/ex_cmds.c in Vim 6.4 and earlier, and 7.x up to 7.1, allows user-assisted remote attackers to execute arbitrary code via format string specifiers in a help-tags tag in a help file, related to the helptags command.	vim	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00115678
10116	CVE-2007-2926	Medium		ISC BIND 9 through 9.5.0a5 uses a weak random number generator during generation of DNS query ids when answering resolver questions or sending NOTIFY messages to slave name servers, which makes it easier for remote attackers to guess the next query id and perform DNS cache poisoning.	bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268315
10117	CVE-2007-2754	Medium		Integer signedness error in truetype/ttgload.c in Freetype 2.3.4 and earlier might allow remote attackers to execute arbitrary code via a crafted TTF image with a negative n_points value, which leads to an integer overflow and heap-based buffer overflow.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268318
10118	CVE-2007-2654	Medium		xfs_fsr in xfsdump creates a .fsr temporary directory with insecure permissions, which allows local users to read or overwrite arbitrary files on xfs filesystems.	xfsdump	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268350
10119	CVE-2007-2445	Medium		The png_handle_tRNS function in pngrutil.c in libpng before 1.0.25 and 1.2.x before 1.2.17 allows remote attackers to cause a denial of service (application crash) via a grayscale PNG image with a bad tRNS chunk CRC value.	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268320
10120	CVE-2007-2438	High		The sandbox for vim allows dangerous functions such as (1) writefile, (2) feedkeys, and (3) system, which might allow user-assisted attackers to execute shell commands and write files via modelines.	vim	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00115677
10121	CVE-2007-2243	Medium		OpenSSH 4.6 and earlier, when ChallengeResponseAuthentication is enabled, allows remote attackers to determine the existence of user accounts by attempting to authenticate via S/KEY, which displays a different response if the user account exists, a similar issue to CVE-2001-1483.	openssh.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231171
10122	CVE-2007-2242	High		The IPv6 protocol allows remote attackers to cause a denial of service via crafted IPv6 type 0 route headers (IPV6_RTHDR_TYPE_0) that create network amplification between two routers.	Linux kernel	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00236403

	A	B	C	D	E	F	G	H	I	J	K	L	M
10123	CVE-2007-2052	Medium		Off-by-one error in the PyLocale_strxfrm function in Modules/_localemodule.c for Python 2.4 and 2.5 causes an incorrect buffer size to be used for the strxfrm function, which allows context-dependent attackers to read portions of memory via unknown manipulations that trigger a buffer over-read due to missing null termination.	python.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268328
10124	CVE-2007-1841	Medium		The isakmp_info_recv function in src/racoon/isakmp_inf.c in racoon in Ipsec-tools before 0.6.7 allows remote attackers to cause a denial of service (tunnel crash) via crafted (1) DELETE (ISAKMP_NPTYPE_D) and (2) NOTIFY (ISAKMP_NPTYPE_N) messages.	ipsec-tools.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268319
10125	CVE-2007-1662	Medium		Perl-Compatible Regular Expression (PCRE) library before 7.3 reads past the end of the string when searching for unmatched brackets and parentheses, which allows context-dependent attackers to cause a denial of service (crash), possibly involving forward references.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118339
10126	CVE-2007-1661	Medium		Perl-Compatible Regular Expression (PCRE) library before 7.3 backtracks too far when matching certain input bytes against some regex patterns in non-UTF-8 mode, which allows context-dependent attackers to obtain sensitive information or cause a denial of service (crash), as demonstrated by the "\X?\d" and "\P{L}?\d" patterns.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118339
10127	CVE-2007-1660	High		Perl-Compatible Regular Expression (PCRE) library before 7.3 does not properly calculate sizes for unspecified "multiple forms of character class" which triggers a buffer overflow that allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118339
10128	CVE-2007-1659	High		Perl-Compatible Regular Expression (PCRE) library before 7.3 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via regex patters containing unmatched "\QIE" sequences with orphan "\E" codes.	pcre	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118339
10129	CVE-2007-1366	Medium		QEMU 0.8.2 allows local users to crash a virtual machine via the divisor operand to the aam instruction, as demonstrated by aam 0x0, which triggers a divide-by-zero error.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00115666
10130	CVE-2007-1351	High		Integer overflow in the bdfReadCharacters function in bdfread.c in (1) X.Org libXfont before 20070403 and (2) freetype 2.3.2 and earlier allows remote authenticated users to execute arbitrary code via crafted BDF fonts, which result in a heap overflow.	freetype.libXfont.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00267984
10131	CVE-2007-1321	Medium		Integer signedness error in the NE2000 emulator in QEMU 0.8.2 allows local users to trigger a heap-based buffer overflow via certain register values that bypass sanity checks, aka QEMU NE2000 "receive" integer signedness error. NOTE: this identifier was inadvertently used by some sources to cover multiple issues that were labeled "NE2000 network driver and the socket code," but separate identifiers have been created for the individual vulnerabilities since there are sometimes different fixes; see CVE-2007-5729 and CVE-2007-5730.	QEMU.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00118334
10132	CVE-2007-1320	High		Multiple heap-based buffer overflows in the cirrus_invalidate_region function in the Cirrus VGA extension in QEMU 0.8.2, as used in Xen and possibly other products, might allow local users to execute arbitrary code via unspecified vectors related to attempting to mark non-existent regions as dirty, aka the bitblt heap overflow.	qemu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00115667
10133	CVE-2007-0822	Low		umount, when running with the Linux 2.6.15 kernel on Slackware Linux 10.2, allows local users to trigger a NULL dereference and application crash by invoking the program with a pathname for a USB pen drive that was mounted and then physically removed, which might allow the users to obtain sensitive information, including core file contents.	umount	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268005
10134	CVE-2007-0494	Medium		ISC BIND 9.0.x, 9.1.x, 9.2.0 up to 9.2.7, 9.3.0 up to 9.3.3, 9.4.0a1 up to 9.4.0a6, 9.4.0b1 up to 9.4.0b4, 9.4.0rc1, and 9.5.0a1 (Bind Forum only) allows remote attackers to cause a denial of service (exit) via a type * (ANY) DNS query response that contains multiple RRsets, which triggers an assertion error, aka the DNSSEC Validation vulnerability.	bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268314
10135	CVE-2007-0493	High		Use-after-free vulnerability in ISC BIND 9.3.0 up to 9.3.3, 9.4.0a1 up to 9.4.0a6, 9.4.0b1 up to 9.4.0b4, 9.4.0rc1, and 9.5.0a1 (Bind Forum only) allows remote attackers to cause a denial of service (named daemon crash) via unspecified vectors that cause named to dereference a freed fetch context.	bind.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00267981
10136	CVE-2006-7254	Low	MEDIUM	The nscd daemon in the GNU C Library (glibc) before version 2.5 does not close incoming client sockets if they cannot be handled by the daemon, allowing local users to carry out a denial of service attack on the daemon.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3897
10137	CVE-2006-7252	Medium		Integer overflow in the calloc function in libc/stdlib/malloc.c in jemalloc in libc for FreeBSD 6.4 and NetBSD makes it easier for context-dependent attackers to perform memory-related attacks such as buffer overflows via a large size value, which triggers a memory allocation of one byte.	libc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00366810
10138	CVE-2006-7250	Medium		The mime_hdr_cmp function in crypto/asn1/asn_mime.c in OpenSSL 0.9.8t and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message.Per: http://cwe.mitre.org/data/definitions/476.html 'CWE-476: NULL Pointer Dereference'	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00337491

	A	B	C	D	E	F	G	H	I	J	K	L	M
10139	CVE-2006-7244	Medium		Memory leak in pngwutil.c in libpng 1.2.13beta1, and other versions before 1.2.15beta3, allows context-dependent attackers to cause a denial of service (memory leak or segmentation fault) via a JPEG image containing an iCCP chunk with a negative embedded profile length.	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00299598
10140	CVE-2006-7243	Medium		PHP before 5.3.4 accepts the \0 character in a pathname, which might allow context-dependent attackers to bypass intended access restrictions by placing a safe file extension after this character, as demonstrated by .php\0.jpg at the end of the argument to the file_exists function.	PHP	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00326010
10141	CVE-2006-7239	Medium		The _gnutls_x509_oid2mac_algorithm function in lib/gnutls_algorithms.c in GnuTLS before 1.4.2 allows remote attackers to cause a denial of service (crash) via a crafted X.509 certificate that uses a hash algorithm that is not supported by GnuTLS, which triggers a NULL pointer dereference.	Gnu gnutls.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00217143
10142	CVE-2006-7236	High		The default configuration of xterm on Debian GNU/Linux sid and possibly Ubuntu enables the allowWindowOps resource, which allows user-assisted attackers to execute arbitrary code or have unspecified other impact via escape sequences.	xterm	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00156703
10143	CVE-2006-7230	Medium		Perl-Compatible Regular Expression (PCRE) library before 7.0 does not properly calculate the amount of memory needed for a compiled regular expression pattern when the (1) -x or (2) -i UTF-8 options change within the pattern, which allows context-dependent attackers to cause a denial of service (PCRE or glibc crash) via crafted regular expressions.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159145
10144	CVE-2006-7229	High		The skge driver 1.5 in Linux kernel 2.6.15 on Ubuntu does not properly use the spin_lock and spin_unlock functions, which allows remote attackers to cause a denial of service (machine crash) via a flood of network traffic.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159240
10145	CVE-2006-7228	Medium		Integer overflow in Perl-Compatible Regular Expression (PCRE) library before 6.7 might allow context-dependent attackers to execute arbitrary code via a regular expression that involves large (1) min, (2) max, or (3) duplength values that cause an incorrect length calculation and trigger a buffer overflow, a different vulnerability than CVE-2006-7227. NOTE: this issue was originally subsumed by CVE-2006-7224, but that CVE has been REJECTED and split.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158920
10146	CVE-2006-7227	Medium		Integer overflow in Perl-Compatible Regular Expression (PCRE) library before 6.7 allows context-dependent attackers to execute arbitrary code via a regular expression containing a large number of named subpatterns (name_count) or long subpattern names (max_name_size), which triggers a buffer overflow. NOTE: this issue was originally subsumed by CVE-2006-7224, but that CVE has been REJECTED and split.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159330
10147	CVE-2006-7226	Medium		Perl-Compatible Regular Expression (PCRE) library before 6.7 does not properly calculate the compiled memory allocation for regular expressions that involve a quantified subpattern containing a named recursion or subroutine reference, which allows context-dependent attackers to cause a denial of service (error or crash).	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159067
10148	CVE-2006-7225	Medium		Perl-Compatible Regular Expression (PCRE) library before 6.7 allows context-dependent attackers to cause a denial of service (error or crash) via a regular expression that involves a malformed POSIX character class, as demonstrated via an invalid character after a [[sequence.	perl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159328
10149	CVE-2006-7203	Medium		The compat_sys_mount function in fs/compat.c in Linux kernel 2.6.20 and earlier allows local users to cause a denial of service (NULL pointer dereference and oops) by mounting a smbfs file system in compatibility mode (mount -t smbfs).	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158916
10150	CVE-2006-7176	Medium		The version of Sendmail 8.13.1-2 on Red Hat Enterprise Linux 4 Update 4 and earlier does not reject the localhost.localdomain domain name for e-mail messages that come from external hosts, which might allow remote attackers to spoof messages.	sendmail	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158993
10151	CVE-2006-7175	High		The version of Sendmail 8.13.1-2 on Red Hat Enterprise Linux 4 Update 4 and earlier does not allow the administrator to disable SSLv2 encryption, which could cause less secure channels to be used than desired.	sendmail	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159151
10152	CVE-2006-7151	Medium		Untrusted search path vulnerability in the libtool-ltdl library (libltdl.so) 1.5.22-2.3 in Fedora Core 5 might allow local users to execute arbitrary code via a malicious library in the (1) hwcap, (2) 0, and (3) nosegneg subdirectories.	libtool	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159331
10153	CVE-2006-7108	Medium		login in util-linux-2.12a skips pam_acct_mgmt and chauth_tok when authentication is skipped, such as when a Kerberos krlogin session has been established, which might allow users to bypass intended access policies that would be enforced by pam_acct_mgmt and chauth_tok.	pam	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159149
10154	CVE-2006-7098	Medium		The Debian GNU/Linux 033_-F_NO_SETSID patch for the Apache HTTP Server 1.3.34-4 does not properly disassociate httpd from a controlling tty when httpd is started interactively, which allows local users to gain privileges to that tty via a CGI program that calls the TIOCSTI ioctl.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159070
10155	CVE-2006-7051	Medium		The sys_timer_create function in posix-timers.c for Linux kernel 2.6.x allows local users to cause a denial of service (memory consumption) and possibly bypass memory limits or cause other processes to be killed by creating a large number of posix timers, which are allocated in kernel memory but are not treated as part of the process' memory.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159073
10156	CVE-2006-6939	Medium		GNU ed before 0.3 allows local users to overwrite arbitrary files via a symlink attack on temporary files, possibly in the open_sbuf function.	gnu	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159237

	A	B	C	D	E	F	G	H	I	J	K	L	M
10157	CVE-2006-6921	Low		Unspecified versions of the Linux kernel allow local users to cause a denial of service (unrecoverable zombie process) via a program with certain instructions that prevent init from properly reaping a child whose parent has died.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159241
10158	CVE-2006-6772	High		Format string vulnerability in the inputAnswer function in file.c in w3m before 0.5.2, when run with the dump or backend option, allows remote attackers to execute arbitrary code via format string specifiers in the Common Name (CN) field of an SSL certificate associated with an https URL.	w3m.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00267989
10159	CVE-2006-6535	High		The dev_queue_xmit function in Linux kernel 2.6 can fail before calling the local_bh_disable function, which could lead to data corruption and node lockups. NOTE: it is not clear whether this issue is exploitable.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00158994
10160	CVE-2006-6493	Medium		Buffer overflow in the krbv4_ldap_auth function in servers/slapd/kerberos.c in OpenLDAP 2.4.3 and earlier, when OpenLDAP is compiled with the --enable-kbind (Kerberos KBIND) option, allows remote attackers to execute arbitrary code via an LDAP bind request using the LDAP_AUTH_KRBV41 authentication method and long credential data.	openldap.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268325
10161	CVE-2006-5794	High		Unspecified vulnerability in the sshd Privilege Separation Monitor in OpenSSH before 4.5 causes weaker verification that authentication has been successful, which might allow attackers to bypass authentication. NOTE: as of 20061108, it is believed that this issue is only exploitable by leveraging vulnerabilities in the unprivileged process, which are not known to exist.	openssh.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231169
10162	CVE-2006-5793	Low		The sPLT chunk handling code (png_set_sPLT function in pngset.c) in libpng 1.0.6 through 1.2.12 uses a sizeof operator on the wrong data type, which allows context-dependent attackers to cause a denial of service (crash) via malformed sPLT chunks that trigger an out-of-bounds read.	libpng.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268004
10163	CVE-2006-5779	Medium		OpenLDAP before 2.3.29 allows remote attackers to cause a denial of service (daemon crash) via LDAP BIND requests with long authcid names, which triggers an assertion failure.	openldap.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268324
10164	CVE-2006-5754	Medium		The aio_setup_ring function in Linux kernel does not properly initialize a variable, which allows local users to cause a denial of service (crash) via an unspecified error path that causes an incorrect free operation.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159235
10165	CVE-2006-5753	High		Unspecified vulnerability in the listxattr system call in Linux kernel, when a bad inode is present, allows local users to cause a denial of service (data corruption) and possibly gain privileges via unknown vectors.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159131
10166	CVE-2006-5752	Medium		Cross-site scripting (XSS) vulnerability in mod_status.c in the mod_status module in Apache HTTP Server (httpd), when ExtendedStatus is enabled and a public server-status page is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving charsets with browsers that perform charset detection when the content-type is not specified.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00159327
10167	CVE-2006-5331			The altivec_unavailable_exception function in arch/powerpc/kernel/traps.c in the Linux kernel before 2.6.19 on 64-bit systems mishandles the case where CONFIG_ALTIVEC is defined and the CPU actually supports Altivec, but the Altivec support was not detected by the kernel, which allows local users to cause a denial of service (panic) by triggering execution of an Altivec instruction.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5679
10168	CVE-2006-5052	Medium		Unspecified vulnerability in portable OpenSSH before 4.4, when running on some platforms, allows remote attackers to determine the validity of usernames via unknown vectors involving a GSSAPI authentication abort.	openssh.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231172
10169	CVE-2006-5051	High		Signal handler race condition in OpenSSH before 4.4 allows remote attackers to cause a denial of service (crash), and possibly execute arbitrary code if GSSAPI authentication is enabled, via unspecified vectors that lead to a double-free.	openssh.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231168
10170	CVE-2006-4925	Medium		packet.c in ssh in OpenSSH allows remote attackers to cause a denial of service (crash) by sending an invalid protocol sequence with USERAUTH_SUCCESS before NEWKEYS, which causes newkeys[mode] to be NULL.	openssh.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231170
10171	CVE-2006-4924	High		sshd in OpenSSH before 4.4, when using the version 1 SSH protocol, allows remote attackers to cause a denial of service (CPU consumption) via an SSH packet that contains duplicate blocks, which is not properly handled by the CRC compensation attack detector.	openssh.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00231166
10172	CVE-2006-4573	Low		Multiple unspecified vulnerabilities in the utf8 combining characters handling (utf8_handle_comb function in encoding.c) in screen before 4.0.3 allows user-assisted attackers to cause a denial of service (crash or hang) via certain UTF8 sequences.	screen.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268007
10173	CVE-2006-3635			The ia64 subsystem in the Linux kernel before 2.6.26 allows local users to cause a denial of service (stack consumption and system crash) via a crafted application that leverages the mishandling of invalid Register Stack Engine (RSE) state.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-5009
10174	CVE-2006-3467	High		Integer overflow in FreeType before 2.2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PCF file, as demonstrated by the Red Hat bad1.pcf test file, due to a partial fix of CVE-2006-1861.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00267982
10175	CVE-2006-2661	Medium		ftutil.c in Freetype before 2.2 allows remote attackers to cause a denial of service (crash) via a crafted font file that triggers a null dereference.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268317

	A	B	C	D	E	F	G	H	I	J	K	L	M
10176	CVE-2006-1861	High		Multiple integer overflows in FreeType before 2.2 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via attack vectors related to (1) bdf/bdflib.c, (2) sfnt/ttcmap.c, (3) cff/cffgload.c, and (4) the read_lwfn function and a crafted LWFN file in base/ttmac.c. NOTE: item 4 was originally identified by CVE-2006-2493.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00267983
10177	CVE-2006-1624	High		The default configuration of syslogd in the Linux sysklogd package does not enable the -x (disable name lookups) option, which allows remote attackers to cause a denial of service (traffic amplification) via messages with spoofed source IP addresses.	sysklogd	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00267988
10178	CVE-2006-0747	Medium		Integer underflow in Freetype before 2.2 allows remote attackers to cause a denial of service (crash) via a font file with an odd number of blue values, which causes the underflow when decrementing by 2 in a context that assumes an even number of values.	freetype.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268316
10179	CVE-2005-4889	High		lib/fsm.c in RPM before 4.4.3 does not properly reset the metadata of an executable file during deletion of the file in an RPM package removal, which might allow local users to gain privileges by creating a hard link to a vulnerable (1) setuid or (2) setgid file, a related issue to CVE-2010-2059.	rpm.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00218809
10180	CVE-2005-4886	High		The selinux_parse_skb_ipv6 function in security/selinux/hooks.c in the Linux kernel before 2.6.12-rc4 allows remote attackers to cause a denial of service (OOPS) via vectors associated with an incorrect call to the ipv6_skip_exthdr function.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00201151
10181	CVE-2005-4881	Medium		The netlink subsystem in the Linux kernel 2.4.x before 2.4.37.6 and 2.6.x before 2.6.13-rc1 does not initialize certain padding fields in structures, which might allow local users to obtain sensitive information from kernel memory via unspecified vectors, related to the (1) tc_fill_qdisc, (2) tcf_fill_node, (3) neightbl_fill_info, (4) neightbl_fill_param_info, (5) neigh_fill_info, (6) rtnetlink_fill_ifinfo, (7) rtnetlink_fill_iwinfo, (8) vif_delete, (9) ipmr_destroy_unres, (10) ipmr_cache_alloc_unres, (11) ipmr_cache_resolve, (12) inet6_fill_ifinfo, (13) tca_get_fill, (14) tca_action_flush, (15) tcf_add_notify, (16) tc_dump_action, (17) cbq_dump_police, (18) __nlmsg_put, (19) __rta_fill, (20) __rta_reserve, (21) inet6_fill_prefix, (22) rsvp_dump, and (23) cbq_dump_ovl functions.	Linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00189679
10182	CVE-2005-3962	Medium		Integer overflow in the format string functionality (Perl_sv_vcatpvfn) in Perl 5.9.2 and 5.8.6 Perl allows attackers to overwrite arbitrary memory and possibly execute arbitrary code via format string specifiers with large values, which causes an integer wrap and leads to a buffer overflow, as demonstrated using format string vulnerabilities in Perl applications.	perl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268327
10183	CVE-2005-3590	High	CRITICAL	The getgrouplist function in the GNU C library (glibc) before version 2.3.5, when invoked with a zero argument, writes to the passed pointer even if the specified array size is zero, leading to a buffer overflow and potentially allowing attackers to corrupt memory.	glibc	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN1018-3898
10184	CVE-2005-2946	Medium		The default configuration on OpenSSL before 0.9.8 uses MD5 for creating message digests instead of a more cryptographically strong algorithm, which makes it easier for remote attackers to forge certificates with a valid certificate authority signature.	openssl.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00268326
10185	CVE-2005-2491	High		Integer overflow in pcre_compile.c in Perl Compatible Regular Expressions (PCRE) before 6.2, as used in multiple products such as Python, Ethereal, and PHP, allows attackers to execute arbitrary code via quantifier values in regular expressions, which leads to a heap-based buffer overflow.	pcre.	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00267987
10186	CVE-2004-2779			id3_utf16_deserialize() in utf16.c in libid3tag through 0.15.1b misparses ID3v2 tags encoded in UTF-16 with an odd number of bytes, triggering an endless loop allocating memory until an OOM condition is reached, leading to denial-of-service (DoS).	libid3tag	Unchanged	8.0.0.26	9.0.0.16	10.17.41.8	10.18.44.1	10.19.45.1	Not vulnerable	LIN10-3343
10187	CVE-2004-1485	High		Buffer overflow in the TFTP client in InetUtils 1.4.2 allows remote malicious DNS servers to execute arbitrary code via a large DNS response that is handled by the gethostbyname function.	InetUtils	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00267985
10188	CVE-2004-0230	MEDIUM		TCP, when using a large Window Size, makes it easier for remote attackers to guess sequence numbers and cause a denial of service (connection loss) to persistent TCP connections by repeatedly injecting a TCP RST packet, especially in protocols that use long-lived connections, such as BGP.	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN8-435
10189	CVE-2003-1605			curl 7.x before 7.10.7 sends CONNECT proxy credentials to the remote server.	curl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN10-4626
10190	CVE-2003-1604	High		The redirect_target function in net/ipv4/netfilter/ipt_REDIRECT.c in the Linux kernel before 2.6.0 allows remote attackers to cause a denial of service (NULL pointer dereference and OOPS) by sending packets to an interface that has a 0.0.0.0 IP address, a related issue to CVE-2015-8787.CWE-476: NULL Pointer Dereference	linux	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-635
10191	CVE-2003-1581	Low		The Apache HTTP Server 2.0.44, when DNS resolution is enabled for client IP addresses, allows remote attackers to inject arbitrary text into log files via an HTTP request in conjunction with a crafted DNS response, as demonstrated by injecting XSS sequences, related to an Inverse Lookup Log Corruption (ILLC) issue.	Apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00200926

	A	B	C	D	E	F	G	H	I	J	K	L	M
10192	CVE-2003-1580	Medium		The Apache HTTP Server 2.0.44, when DNS resolution is enabled for client IP addresses, uses a logging format that does not identify whether a dotted quad represents an unresolved IP address, which allows remote attackers to spoof IP addresses via crafted DNS responses containing numerical top-level domains, as demonstrated by a forged 123.123.123.123 domain name, related to an Inverse Lookup Log Corruption (ILLC) issue.	apache	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00200923
10193	CVE-2002-2443	Medium		schpw.c in the kpasswd service in kadmind in MIT Kerberos 5 (aka krb5) before 1.11.3 does not properly validate UDP packets before sending responses, which allows remote attackers to cause a denial of service (CPU and bandwidth consumption) via a forged packet that triggers a communication loop, as demonstrated by krb_pingpong.nasl, a related issue to CVE-1999-0103.	krb5	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	WIND00419898
10194	CVE-2000-1254	Medium		crypto/rsa/rsa_gen.c in OpenSSL before 0.9.6 mishandles C bitwise-shift operations that exceed the size of an expression, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by leveraging improper RSA key generation on 64-bit HP-UX platforms.	openssl	Unchanged	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	Not vulnerable	LIN9-663