Lumeta ESI 4.0 Security Page

This page shows the package changes from 3.3.5.1 to 4.0 some for security reasons and the CVEs.

Upgrade to 3.3.6 is allowed from any 3.3.5.*. To upgrade to version 4.0, customers must save a backup and restore the backup on a fresh install of 4.0.

Version 3.3.6 has no security updates from 3.3.5.1. This page shows only the changes from 3.3.5.1 to 4.0.

Deliverable	Name
netboot/isoboot	esi-4.0
upgrade	*none*

CVEs and the new package and RPM that resolves each.

CVE	New RPM	PKG	DESCRIPTION
CVE-2014-9112	cpio-2.11-27.el7.x86_64	cpio	Heap-based buffer overflow in the process_copy_in function in GNU Cpio 2.11 allows remote attackers to ca large block value in a cpio archive.
CVE-2013-2168	dbus-1.10.24-13.el7_6.x86_64	dbus	The _dbus_printf_string_upper_bound function in dbus/dbus-sysdeps-unix.c in D-Bus (aka DBus) 1.4.x befo and 1.7.x before 1.7.4 allows local users to cause a denial of service (service crash) via a crafted message.
CVE-2013-2168	dbus-libs-1.10.24-13.el7_6.x86_64	dbus-libs	The _dbus_printf_string_upper_bound function in dbus/dbus-sysdeps-unix.c in D-Bus (aka DBus) 1.4.x befo and 1.7.x before 1.7.4 allows local users to cause a denial of service (service crash) via a crafted message.
CVE-2019-7150	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	An issue was discovered in elfutils 0.175. A segmentation fault can occur in the function elf64_xlatetom in lib dwfl_segment_report_module not checking whether the dyn data read from a core file is truncated. A crafted crash, leading to denial-of-service, as demonstrated by eu-stack.
CVE-2019-7150	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	An issue was discovered in elfutils 0.175. A segmentation fault can occur in the function elf64_xlatetom in lib dwfl_segment_report_module not checking whether the dyn data read from a core file is truncated. A crafted crash, leading to denial-of-service, as demonstrated by eu-stack.
CVE-2011-4868	dhclient-4.2.5-77.el7.centos.x86_64	dhclient	The logging functionality in dhcpd in ISC DHCP before 4.2.3-P2, when using Dynamic DNS (DDNS) and issu properly handle the DHCPv6 lease structure, which allows remote attackers to cause a denial of service (NU daemon crash) via crafted packets related to a lease-status update.
CVE-2011-4868	dhcp-common-4.2.5-77.el7.centos.x86_64	dhcp-common	The logging functionality in dhcpd in ISC DHCP before 4.2.3-P2, when using Dynamic DNS (DDNS) and issu properly handle the DHCPv6 lease structure, which allows remote attackers to cause a denial of service (NU daemon crash) via crafted packets related to a lease-status update.
CVE-2018-16062	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	dwarf_getaranges in dwarf_getaranges.c in libdw in elfutils before 2018-08-18 allows remote attackers to cau (heap-based buffer over-read) via a crafted file.
CVE-2018-16062	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	dwarf_getaranges in dwarf_getaranges.c in libdw in elfutils before 2018-08-18 allows remote attackers to cau (heap-based buffer over-read) via a crafted file.
CVE-2016-2774	dhclient-4.2.5-77.el7.centos.x86_64	dhclient	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 concu allows remote attackers to cause a denial of service (INSIST assertion failure or request-processing outage)
CVE-2016-2774	dhcp-common-4.2.5-77.el7.centos.x86_64	dhcp-common	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 concu allows remote attackers to cause a denial of service (INSIST assertion failure or request-processing outage)
CVE-2019-7149	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	A heap-based buffer over-read was discovered in the function read_srclines in dwarf_getsrclines.c in libdw ir can cause segmentation faults, leading to denial-of-service, as demonstrated by eu-nm.
CVE-2019-7149	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	A heap-based buffer over-read was discovered in the function read_srclines in dwarf_getsrclines.c in libdw ir can cause segmentation faults, leading to denial-of-service, as demonstrated by eu-nm.
CVE-2018-18310	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	An invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl in elfutil vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file, as demo
CVE-2018-18310	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	An invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl in elfutil vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file, as demo
CVE-2015-2716	expat-2.1.0-11.el7.x86_64	expat	Buffer overflow in the XML parser in Mozilla Firefox before 38.0, Firefox ESR 31.x before 31.7, and Thunderl attackers to execute arbitrary code by providing a large amount of compressed XML data, a related issue to
CVE-2018-16403	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	libdw in elfutils 0.173 checks the end of the attributes list incorrectly in dwarf_getabbrev in dwarf_getabbrev.c dwarf_hasattr.c, leading to a heap-based buffer over-read and an application crash.

CVE-2018-16403	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	libdw in elfutils 0.173 checks the end of the attributes list incorrectly in dwarf_getabbrev in dwarf_getabbrev.c dwarf_hasattr.c, leading to a heap-based buffer over-read and an application crash.
CVE-2012-3570	dhclient-4.2.5-77.el7.centos.x86_64	dhclient	Buffer overflow in ISC DHCP 4.2.x before 4.2.4-P1, when DHCPv6 mode is enabled, allows remote attackers (segmentation fault and daemon exit) via a crafted client identifier parameter.
CVE-2012-3570	dhcp-common-4.2.5-77.el7.centos.x86_64	dhcp-common	Buffer overflow in ISC DHCP 4.2.x before 4.2.4-P1, when DHCPv6 mode is enabled, allows remote attackers (segmentation fault and daemon exit) via a crafted client identifier parameter.
CVE-2019-7148	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	An attempted excessive memory allocation was discovered in the function read_long_names in elf_begin.c in attackers could leverage this vulnerability to cause a denial-of-service via crafted elf input, which leads to an NOTE: The maintainers believe this is not a real issue, but instead a "warning caused by ASAN because the ASAN_OPTIONS=allocator_may_return_null=1 and running the reproducer, nothing happens."
CVE-2019-7148	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	An attempted excessive memory allocation was discovered in the function read_long_names in elf_begin.c in attackers could leverage this vulnerability to cause a denial-of-service via crafted elf input, which leads to an NOTE: The maintainers believe this is not a real issue, but instead a "warning caused by ASAN because the ASAN_OPTIONS=allocator_may_return_null=1 and running the reproducer, nothing happens."
CVE-2010-3616	dhclient-4.2.5-77.el7.centos.x86_64	dhclient	ISC DHCP server 4.2 before 4.2.0-P2, when configured to use failover partnerships, allows remote attackers (communications-interrupted state and DHCP client service loss) by connecting to a port that is only intended demonstrated by a Nagios check_tcp process check to TCP port 520.
CVE-2010-3616	dhcp-common-4.2.5-77.el7.centos.x86_64	dhcp-common	ISC DHCP server 4.2 before 4.2.0-P2, when configured to use failover partnerships, allows remote attackers (communications-interrupted state and DHCP client service loss) by connecting to a port that is only intended demonstrated by a Nagios check_tcp process check to TCP port 520.
CVE-2019-7146	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	In elfutils 0.175, there is a buffer over-read in the ebl_object_note function in eblobjnote.c in libebl. Remote a vulnerability to cause a denial-of-service via a crafted elf file, as demonstrated by eu-readelf.
CVE-2019-7146	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	In elfutils 0.175, there is a buffer over-read in the ebl_object_note function in eblobjnote.c in libebl. Remote a vulnerability to cause a denial-of-service via a crafted elf file, as demonstrated by eu-readelf.
CVE-2018-18521	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	Divide-by-zero vulnerabilities in the function arlib_add_symbols() in arlib.c in elfutils 0.174 allow remote attac service (application crash) with a crafted ELF file, as demonstrated by eu-ranlib, because a zero sh_entsize i
CVE-2018-18521	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	Divide-by-zero vulnerabilities in the function arlib_add_symbols() in arlib.c in elfutils 0.174 allow remote attac service (application crash) with a crafted ELF file, as demonstrated by eu-ranlib, because a zero sh_entsize i
CVE-2019-7664	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	In elfutils 0.175, a negative-sized memcpy is attempted in elf_cvt_note in libelf/note_xlate.h because of an in elf input causes a segmentation fault, leading to denial of service (program crash).
CVE-2019-7664	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	In elfutils 0.175, a negative-sized memcpy is attempted in elf_cvt_note in libelf/note_xlate.h because of an in elf input causes a segmentation fault, leading to denial of service (program crash).
CVE-2018-16402	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	libelf/elf_end.c in elfutils 0.173 allows remote attackers to cause a denial of service (double free and applicat unspecified other impact because it tries to decompress twice.
CVE-2018-16402	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	libelf/elf_end.c in elfutils 0.173 allows remote attackers to cause a denial of service (double free and applicat unspecified other impact because it tries to decompress twice.
CVE-2018-18520	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	An Invalid Memory Address Dereference exists in the function elf_end in libelf in elfutils through v0.174. Alth support ar files inside ar files, handle_ar in size.c closes the outer ar file before handling all inner entries. The to cause a denial of service (application crash) with a crafted ELF file.
CVE-2018-18520	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	An Invalid Memory Address Dereference exists in the function elf_end in libelf in elfutils through v0.174. Alth support ar files inside ar files, handle_ar in size.c closes the outer ar file before handling all inner entries. The to cause a denial of service (application crash) with a crafted ELF file.
CVE-2019-7665	elfutils-libelf-0.176-2.el7.x86_64	elfutils-libelf	In elfutils 0.175, a heap-based buffer over-read was discovered in the function elf32_xlatetom in elf32_xlatet input can cause a segmentation fault leading to denial of service (program crash) because ebl_core_note do file notes.
CVE-2019-7665	elfutils-libs-0.176-2.el7.x86_64	elfutils-libs	In elfutils 0.175, a heap-based buffer over-read was discovered in the function elf32_xlatetom in elf32_xlatet input can cause a segmentation fault leading to denial of service (program crash) because ebl_core_note do file notes.
CVE-2017-7488	authconfig-6.2.8-30.el7.x86_64	authconfig	Authconfig version 6.2.8 is vulnerable to an Information exposure while using SSSD to authenticate against r leak of information about existing usernames.
CVE-2010-2526	device-mapper-1.02.158-2.el7.x86_64	device-mapper	The cluster logical volume manager daemon (clvmd) in lvm2-cluster in LVM2 before 2.02.72, as used in Red and other products, does not verify client credentials upon a socket connection, which allows local users to c (daemon exit or logical-volume change) or possibly have unspecified other impact via crafted control comma
CVE-2010-2526	device-mapper-event-1.02.158-2.el7.x86_64	device-mapper-event	The cluster logical volume manager daemon (clvmd) in lvm2-cluster in LVM2 before 2.02.72, as used in Red and other products, does not verify client credentials upon a socket connection, which allows local users to c (daemon exit or logical-volume change) or possibly have unspecified other impact via crafted control comma
CVE-2010-2526	device-mapper-event-libs-1.02.158-2.el7.x86_64	device-mapper-event-libs	The cluster logical volume manager daemon (clvmd) in lvm2-cluster in LVM2 before 2.02.72, as used in Red and other products, does not verify client credentials upon a socket connection, which allows local users to c (daemon exit or logical-volume change) or possibly have unspecified other impact via crafted control comma
CVE-2010-2526	device-mapper-libs-1.02.158-2.el7.x86_64	device-mapper-libs	The cluster logical volume manager daemon (clvmd) in lvm2-cluster in LVM2 before 2.02.72, as used in Red and other products, does not verify client credentials upon a socket connection, which allows local users to c (daemon exit or logical-volume change) or possibly have unspecified other impact via crafted control comma
CVE-2010-2526	lvm2-2.02.185-2.el7.x86_64	lvm2	The cluster logical volume manager daemon (clvmd) in lvm2-cluster in LVM2 before 2.02.72, as used in Red and other products, does not verify client credentials upon a socket connection, which allows local users to c (daemon exit or logical-volume change) or possibly have unspecified other impact via crafted control comma

CVE-2010-2526	lvm2-libs-2.02.185-2.el7.x86_64	lvm2-libs	The cluster logical volume manager daemon (clvmd) in lvm2-cluster in LVM2 before 2.02.72, as used in Red and other products, does not verify client credentials upon a socket connection, which allows local users to c (daemon exit or logical-volume change) or possibly have unspecified other impact via crafted control comma
CVE-2011-2896	cups-libs-1.6.3-40.el7.x86_64	cups-libs	The LZW decompressor in the LWZReadByte function in giftoppm.c in the David Koblas GIF decoder in PBM gif_read_lzw function in filter/image-gif.c in CUPS before 1.4.7, the LZWReadByte function in plug-ins/comm and earlier, the LZWReadByte function in img/gifread.c in XPCE in SWI-Prolog 5.10.4 and earlier, and other handle code words that are absent from the decompression table when encountered, which allows remote at loop or a heap-based buffer overflow, and possibly execute arbitrary code, via a crafted compressed stream, CVE-2006-1168 and CVE-2011-2895.
CVE-2018-1000122	curl-7.29.0-54.el7.x86_64	curl	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allo of service or information leakage
CVE-2018-1000122	libcurl-7.29.0-54.el7.x86_64	libcurl	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allo of service or information leakage
CVE-2016-5420	curl-7.29.0-54.el7.x86_64	curl	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, attackers to hijack the authentication of the connection by leveraging a previously created connection with a
CVE-2016-5420	libcurl-7.29.0-54.el7.x86_64	libcurl	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, attackers to hijack the authentication of the connection by leveraging a previously created connection with a
CVE-2018-14618	curl-7.29.0-54.el7.x86_64	curl	curl before version 7.61.1 is vulnerable to a buffer overrun in the NTLM authentication code. The internal fun Curl_ntlm_core_mk_nt_hash multiplies the length of the password by two (SUM) to figure out how large tem from the heap. The length value is then subsequently used to iterate over the password and generate output buffer. On systems with a 32 bit size_t, the math to calculate SUM triggers an integer overflow when the pas (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the making the use of that buffer end up in a heap buffer overflow. (This bug is almost identical to CVE-2017-881
CVE-2018-14618	libcurl-7.29.0-54.el7.x86_64	libcurl	curl before version 7.61.1 is vulnerable to a buffer overrun in the NTLM authentication code. The internal fun Curl_ntlm_core_mk_nt_hash multiplies the length of the password by two (SUM) to figure out how large tem from the heap. The length value is then subsequently used to iterate over the password and generate output buffer. On systems with a 32 bit size_t, the math to calculate SUM triggers an integer overflow when the pas (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the making the use of that buffer end up in a heap buffer overflow. (This bug is almost identical to CVE-2017-881
CVE-2018-1000301	curl-7.29.0-54.el7.x86_64	curl	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in de curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.
CVE-2018-1000301	libcurl-7.29.0-54.el7.x86_64	libcurl	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in de curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.
CVE-2018-1000121	curl-7.29.0-54.el7.x86_64	curl	A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an service
CVE-2018-1000121	libcurl-7.29.0-54.el7.x86_64	libcurl	A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an service
CVE-2018-1000120	curl-7.29.0-54.el7.x86_64	curl	A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an atta service or worse.
CVE-2018-1000120	libcurl-7.29.0-54.el7.x86_64	libcurl	A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an atta service or worse.
CVE-2012-0036	curl-7.29.0-54.el7.x86_64	curl	curl and libcurl 7.2x before 7.24.0 do not properly consider special characters during extraction of a pathnam remote attackers to conduct data-injection attacks via a crafted URL, as demonstrated by a CRLF injection a POP3, or (3) SMTP protocol.
CVE-2012-0036	libcurl-7.29.0-54.el7.x86_64	libcurl	curl and libcurl 7.2x before 7.24.0 do not properly consider special characters during extraction of a pathnam remote attackers to conduct data-injection attacks via a crafted URL, as demonstrated by a CRLF injection a POP3, or (3) SMTP protocol.
CVE-2017-1000257	curl-7.29.0-54.el7.x86_64	curl	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that respon libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function. lib treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or ju to the application as if it was actually downloaded.
CVE-2017-1000257	libcurl-7.29.0-54.el7.x86_64	libcurl	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that respon libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function. lib treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or ju to the application as if it was actually downloaded.
CVE-2013-0249	curl-7.29.0-54.el7.x86_64	curl	Stack-based buffer overflow in the Curl_sasl_create_digest_md5_message function in lib/curl_sasl.c in curl a 7.28.1, when negotiating SASL DIGEST-MD5 authentication, allows remote attackers to cause a denial of se execute arbitrary code via a long string in the realm parameter in a (1) POP3, (2) SMTP or (3) IMAP messag
CVE-2013-0249	libcurl-7.29.0-54.el7.x86_64	libcurl	Stack-based buffer overflow in the Curl_sasl_create_digest_md5_message function in lib/curl_sasl.c in curl a 7.28.1, when negotiating SASL DIGEST-MD5 authentication, allows remote attackers to cause a denial of se execute arbitrary code via a long string in the realm parameter in a (1) POP3, (2) SMTP or (3) IMAP messag
CVE-2016-7167	curl-7.29.0-54.el7.x86_64	curl	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-
CVE-2016-7167	libcurl-7.29.0-54.el7.x86_64	libcurl	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-

CVE-2018-16842	curl-7.29.0-54.el7.x86_64	curl	Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the tool_msgs.c:voutf information exposure and denial of service.
CVE-2018-16842	libcurl-7.29.0-54.el7.x86_64	libcurl	Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the tool_msgs.c:voutf information exposure and denial of service.
CVE-2018-1000007	curl-7.29.0-54.el7.x86_64	curl	libcurl 7.1 through 7.57.0 might accidentally leak authentication data to third parties. When asked to send cus requests, libcurl will send that set of headers first to the host in the initial URL but also, if asked to follow redi response code is returned, to the host mentioned in URL in the `Location:` response header value. Sending t subsequent hosts is in particular a problem for applications that pass on custom `Authorization:` headers, as privacy sensitive information or data that could allow others to impersonate the libcurl-using client's request.
CVE-2018-1000007	libcurl-7.29.0-54.el7.x86_64	libcurl	libcurl 7.1 through 7.57.0 might accidentally leak authentication data to third parties. When asked to send cus requests, libcurl will send that set of headers first to the host in the initial URL but also, if asked to follow redi response code is returned, to the host mentioned in URL in the `Location:` response header value. Sending t subsequent hosts is in particular a problem for applications that pass on custom `Authorization:` headers, as privacy sensitive information or data that could allow others to impersonate the libcurl-using client's request.
CVE-2016-5419	curl-7.29.0-54.el7.x86_64	curl	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed to bypass intended restrictions by resuming a session.
CVE-2016-5419	libcurl-7.29.0-54.el7.x86_64	libcurl	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed to bypass intended restrictions by resuming a session.
CVE-2018-18751	gettext-0.19.8.1-3.el7.x86_64	gettext	An issue was discovered in GNU gettext 0.19.8. There is a double free in default_add_message in read-cata in po_gram_parse in po-gram-gen.y, as demonstrated by lt-msgfmt.
CVE-2013-0242	glibc-2.17-292.el7.x86_64	glibc	Buffer overflow in the extend_buffers function in the regularexpression matcher (posix/regexec.c) in glibc, po context-dependent attackers to cause a denial of service (memory corruption and crash) via crafted multibyte
CVE-2013-0242	glibc-common-2.17-292.el7.x86_64	glibc-common	Buffer overflow in the extend_buffers function in the regularexpression matcher (posix/regexec.c) in glibc, po context-dependent attackers to cause a denial of service (memory corruption and crash) via crafted multibyte
CVE-2016-5384	fontconfig-2.13.0-4.3.el7.x86_64	fontconfig	fontconfig before 2.12.1 does not validate offsets, which allows local users to trigger arbitrary free calls and c free attacks and execute arbitrary code via a crafted cache file.
CVE-2016-3706	glibc-2.17-292.el7.x86_64	glibc	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in the GNU C Library (remote attackers to cause a denial of service (crash) via vectors involving hostent conversion. NOTE: this vu incomplete fix for CVE-2013-4458.
CVE-2016-3706	glibc-common-2.17-292.el7.x86_64	glibc-common	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in the GNU C Library (remote attackers to cause a denial of service (crash) via vectors involving hostent conversion. NOTE: this vu incomplete fix for CVE-2013-4458.
CVE-2014-3478	file-5.11-35.el7.x86_64	file	Buffer overflow in the mconvert function in softmagic.c in file before 5.19, as used in the Fileinfo component i before 5.5.14, allows remote attackers to cause a denial of service (application crash) via a crafted Pascal st conversion.
CVE-2014-3478	file-libs-5.11-35.el7.x86_64	file-libs	Buffer overflow in the mconvert function in softmagic.c in file before 5.19, as used in the Fileinfo component i before 5.5.14, allows remote attackers to cause a denial of service (application crash) via a crafted Pascal st conversion.
CVE-2014-8121	glibc-2.17-292.el7.x86_64	glibc	DB_LOOKUP in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6 properly check if a file is open, which allows remote attackers to cause a denial of service (infinite loop) by pe database while iterating over it, which triggers the file pointer to be reset.
CVE-2014-8121	glibc-common-2.17-292.el7.x86_64	glibc-common	DB_LOOKUP in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6 properly check if a file is open, which allows remote attackers to cause a denial of service (infinite loop) by pe database while iterating over it, which triggers the file pointer to be reset.
CVE-2012-4424	glibc-2.17-292.el7.x86_64	glibc	Stack-based buffer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allow to cause a denial of service (crash) or possibly execute arbitrary code via a long string that triggers a malloc function.
CVE-2012-4424	glibc-common-2.17-292.el7.x86_64	glibc-common	Stack-based buffer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allow to cause a denial of service (crash) or possibly execute arbitrary code via a long string that triggers a malloc function.
CVE-2010-3847	glibc-2.17-292.el7.x86_64	glibc	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 $ORIGIN for the LD_AUDIT environment variable, which allows local users to gain privileges via a crafted dy located in an arbitrary directory.
CVE-2010-3847	glibc-common-2.17-292.el7.x86_64	glibc-common	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 $ORIGIN for the LD_AUDIT environment variable, which allows local users to gain privileges via a crafted dy located in an arbitrary directory.
CVE-2014-0207	file-5.11-35.el7.x86_64	file	The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP bef 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a craft
CVE-2014-0207	file-libs-5.11-35.el7.x86_64	file-libs	The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP bef 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a craft
CVE-2015-5229	glibc-2.17-292.el7.x86_64	glibc	The calloc function in the glibc package in Red Hat Enterprise Linux (RHEL) 6.7 and 7.2 does not properly in might allow context-dependent attackers to cause a denial of service (hang or crash) via unspecified vectors.
CVE-2015-5229	glibc-common-2.17-292.el7.x86_64	glibc-common	The calloc function in the glibc package in Red Hat Enterprise Linux (RHEL) 6.7 and 7.2 does not properly in might allow context-dependent attackers to cause a denial of service (hang or crash) via unspecified vectors.

CVE-2013-7423	glibc-2.17-292.el7.x86_64	glibc	The send_dg function in resolv/res_send.c in GNU C Library (aka glibcor libc6) before 2.20 does not properly allows remote attackers to send DNS queries to unintended locations via a large number of request that trigg function.
CVE-2013-7423	glibc-common-2.17-292.el7.x86_64	glibc-common	The send_dg function in resolv/res_send.c in GNU C Library (aka glibcor libc6) before 2.20 does not properly allows remote attackers to send DNS queries to unintended locations via a large number of request that trigg function.
CVE-2014-5119	glibc-2.17-292.el7.x86_64	glibc	Off-by-one error in the __gconv_translit_find function ingconv_trans.c in GNU C Library (aka glibc) allows co cause a denial of service (crash) or execute arbitrary code via vectors related to the CHARSET environment transliteration modules.
CVE-2014-5119	glibc-common-2.17-292.el7.x86_64	glibc-common	Off-by-one error in the __gconv_translit_find function ingconv_trans.c in GNU C Library (aka glibc) allows co cause a denial of service (crash) or execute arbitrary code via vectors related to the CHARSET environment transliteration modules.
CVE-2013-4332	glibc-2.17-292.el7.x86_64	glibc	Multiple integer overflows in malloc/malloc.c in the GNU C Library (aka glibc or libc6) 2.18 and earlier allow c cause a denial of service (heap corruption) via a large value to the (1) pvalloc, (2) valloc, (3) posix_memalign aligned_alloc functions.
CVE-2013-4332	glibc-common-2.17-292.el7.x86_64	glibc-common	Multiple integer overflows in malloc/malloc.c in the GNU C Library (aka glibc or libc6) 2.18 and earlier allow c cause a denial of service (heap corruption) via a large value to the (1) pvalloc, (2) valloc, (3) posix_memalign aligned_alloc functions.
CVE-2018-11236	glibc-2.17-292.el7.x86_64	glibc	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pa realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffe arbitrary code execution.
CVE-2018-11236	glibc-common-2.17-292.el7.x86_64	glibc-common	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pa realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffe arbitrary code execution.
CVE-2015-7547	glibc-2.17-292.el7.x86_64	glibc	Multiple stack-based buffer overflows in the (1) send_dg and (2)send_vc functions in the libresolv library in th libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary co that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to p queries" and the libnss_dns.so.2 NSS module.
CVE-2015-7547	glibc-common-2.17-292.el7.x86_64	glibc-common	Multiple stack-based buffer overflows in the (1) send_dg and (2)send_vc functions in the libresolv library in th libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary co that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to p queries" and the libnss_dns.so.2 NSS module.
CVE-2012-4412	glibc-2.17-292.el7.x86_64	glibc	Integer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-d denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a heap-based buf
CVE-2012-4412	glibc-common-2.17-292.el7.x86_64	glibc-common	Integer overflow in string/strcoll_l.c in the GNU C Library (aka glibc or libc6) 2.17 and earlier allows context-d denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a heap-based buf
CVE-2016-3075	glibc-2.17-292.el7.x86_64	glibc	Stack-based buffer overflow in the nss_dns implementation of the getnetbyname function in GNU C Library (context-dependent attackers to cause a denial of service (stack consumption and application crash) via a lon
CVE-2016-3075	glibc-common-2.17-292.el7.x86_64	glibc-common	Stack-based buffer overflow in the nss_dns implementation of the getnetbyname function in GNU C Library (context-dependent attackers to cause a denial of service (stack consumption and application crash) via a lon
CVE-2014-6040	glibc-2.17-292.el7.x86_64	glibc	GNU C Library (aka glibc) before 2.20 allows context-dependentattackers to cause a denial of service (out-of multibyte character value of "0xffff" to the iconv function when converting (1) IBM933, (2) IBM935, (3) IBM93 encoded data to UTF-8.
CVE-2014-6040	glibc-common-2.17-292.el7.x86_64	glibc-common	GNU C Library (aka glibc) before 2.20 allows context-dependentattackers to cause a denial of service (out-of multibyte character value of "0xffff" to the iconv function when converting (1) IBM933, (2) IBM935, (3) IBM93 encoded data to UTF-8.
CVE-2015-0235	glibc-2.17-292.el7.x86_64	glibc	Heap-based buffer overflow in the __nss_hostname_digits_dots functionin glibc 2.2, and other 2.x versions b context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) get "GHOST."
CVE-2015-0235	glibc-common-2.17-292.el7.x86_64	glibc-common	Heap-based buffer overflow in the __nss_hostname_digits_dots functionin glibc 2.2, and other 2.x versions b context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) get "GHOST."
CVE-2018-1000001	glibc-2.17-292.el7.x86_64	glibc	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write l leading to a buffer underflow and potential code execution.
CVE-2018-1000001	glibc-common-2.17-292.el7.x86_64	glibc-common	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write l leading to a buffer underflow and potential code execution.
CVE-2013-4458	glibc-2.17-292.el7.x86_64	glibc	Stack-based buffer overflow in the getaddrinfo function insysdeps/posix/getaddrinfo.c in GNU C Library (aka allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers address results. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-1914.
CVE-2013-4458	glibc-common-2.17-292.el7.x86_64	glibc-common	Stack-based buffer overflow in the getaddrinfo function insysdeps/posix/getaddrinfo.c in GNU C Library (aka allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers address results. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-1914.
CVE-2015-1473	glibc-2.17-292.el7.x86_64	glibc	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not p during a risk-management decision for use of the alloca function, which might allow context-dependent attacl service (segmentation violation) or overwrite memory locations beyond the stack boundary via a long line co are improperly handled in a wscanf call.

CVE-2015-1473	glibc-common-2.17-292.el7.x86_64	glibc-common	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not p during a risk-management decision for use of the alloca function, which might allow context-dependent attac service (segmentation violation) or overwrite memory locations beyond the stack boundary via a long line co are improperly handled in a wscanf call.
CVE-2017-16997	glibc-2.17-292.el7.x86_64	glibc	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH c privileged (setuid or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse lib directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion o token as the "./" directory. NOTE: this configuration of RPATH/RUNPATH for a privileged program is appare likely, no such program is shipped with any common Linux distribution.
CVE-2017-16997	glibc-common-2.17-292.el7.x86_64	glibc-common	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH c privileged (setuid or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse lib directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion o token as the "./" directory. NOTE: this configuration of RPATH/RUNPATH for a privileged program is appare likely, no such program is shipped with any common Linux distribution.
CVE-2014-9402	glibc-2.17-292.el7.x86_64	glibc	The nss_dns implementation of getnetbyname in GNU C Library (aka glibc) before 2.21, when the DNS back Switch configuration is enabled, allows remote attackers to cause a denial of service (infinite loop) by sendin network name is being process.
CVE-2014-9402	glibc-common-2.17-292.el7.x86_64	glibc-common	The nss_dns implementation of getnetbyname in GNU C Library (aka glibc) before 2.21, when the DNS back Switch configuration is enabled, allows remote attackers to cause a denial of service (infinite loop) by sendin network name is being process.
CVE-2013-1914	glibc-2.17-292.el7.x86_64	glibc	Stack-based buffer overflow in the getaddrinfo function insysdeps/posix/getaddrinfo.c in GNU C Library (aka allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers conversion results.
CVE-2013-1914	glibc-common-2.17-292.el7.x86_64	glibc-common	Stack-based buffer overflow in the getaddrinfo function insysdeps/posix/getaddrinfo.c in GNU C Library (aka allows remote attackers to cause a denial of service (crash) via a (1) hostname or (2) IP address that triggers conversion results.
CVE-2017-15804	glibc-2.17-292.el7.x86_64	glibc	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow du with the ~ operator.
CVE-2017-15804	glibc-common-2.17-292.el7.x86_64	glibc-common	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow du with the ~ operator.
CVE-2010-3856	glibc-2.17-292.el7.x86_64	glibc	ld.so in the GNU C Library (aka glibc or libc6) before 2.11.3, and2.12.x before 2.12.2, does not properly restr environment variable to reference dynamic shared objects (DSOs) as audit objects, which allows local users an unsafe DSO located in a trusted library directory, as demonstrated by libpcprofile.so.
CVE-2010-3856	glibc-common-2.17-292.el7.x86_64	glibc-common	ld.so in the GNU C Library (aka glibc or libc6) before 2.11.3, and2.12.x before 2.12.2, does not properly restr environment variable to reference dynamic shared objects (DSOs) as audit objects, which allows local users an unsafe DSO located in a trusted library directory, as demonstrated by libpcprofile.so.
CVE-2015-8776	glibc-2.17-292.el7.x86_64	glibc	The strftime function in the GNU C Library (aka glibc or libc6) before2.23 allows context-dependent attackers (application crash) or possibly obtain sensitive information via an out-of-range time value.
CVE-2015-8776	glibc-common-2.17-292.el7.x86_64	glibc-common	The strftime function in the GNU C Library (aka glibc or libc6) before2.23 allows context-dependent attackers (application crash) or possibly obtain sensitive information via an out-of-range time value.
CVE-2017-15670	glibc-2.17-292.el7.x86_64	glibc	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buff in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
CVE-2017-15670	glibc-common-2.17-292.el7.x86_64	glibc-common	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buff in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
CVE-2015-5277	glibc-2.17-292.el7.x86_64	glibc	The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS fil
CVE-2015-5277	glibc-common-2.17-292.el7.x86_64	glibc-common	The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS fil
CVE-2013-4788	glibc-2.17-292.el7.x86_64	glibc	The PTR_MANGLE implementation in the GNU C Library (aka glibc or libc6) 2.4, 2.17, and earlier, and Emb not initialize the random value for the pointer guard, which makes it easier for context-dependent attackers to leveraging a buffer-overflow vulnerability in an application and using the known zero value pointer guard to c
CVE-2013-4788	glibc-common-2.17-292.el7.x86_64	glibc-common	The PTR_MANGLE implementation in the GNU C Library (aka glibc or libc6) 2.4, 2.17, and earlier, and Emb not initialize the random value for the pointer guard, which makes it easier for context-dependent attackers to leveraging a buffer-overflow vulnerability in an application and using the known zero value pointer guard to c
CVE-2018-11237	glibc-2.17-292.el7.x86_64	glibc	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.2 beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.
CVE-2018-11237	glibc-common-2.17-292.el7.x86_64	glibc-common	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.2 beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.
CVE-2014-3487	file-5.11-35.el7.x86_64	file	The cdf_read_property_info function in file before 5.19, as used in the Fileinfo component in PHP before 5.4. does not properly validate a stream offset, which allows remote attackers to cause a denial of service (applic file.
CVE-2014-3487	file-libs-5.11-35.el7.x86_64	file-libs	The cdf_read_property_info function in file before 5.19, as used in the Fileinfo component in PHP before 5.4. does not properly validate a stream offset, which allows remote attackers to cause a denial of service (applic file.

CVE-2015-1781	glibc-2.17-292.el7.x86_64	glibc	Buffer overflow in the gethostbyname_r and other unspecified NSSfunctions in the GNU C Library (aka glibc context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS with a misaligned buffer.
CVE-2015-1781	glibc-common-2.17-292.el7.x86_64	glibc-common	Buffer overflow in the gethostbyname_r and other unspecified NSSfunctions in the GNU C Library (aka glibc context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS with a misaligned buffer.
CVE-2016-10739	glibc-2.17-292.el7.x86_64	glibc	In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a st address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.
CVE-2016-10739	glibc-common-2.17-292.el7.x86_64	glibc-common	In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a st address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.
CVE-2013-4237	glibc-2.17-292.el7.x86_64	glibc	sysdeps/posix/readdir_r.c in the GNU C Library (aka glibc or libc6)2.18 and earlier allows context-dependent service (out-of-bounds write and crash) or possibly execute arbitrary code via a crafted (1) NTFS or (2) CIFS
CVE-2013-4237	glibc-common-2.17-292.el7.x86_64	glibc-common	sysdeps/posix/readdir_r.c in the GNU C Library (aka glibc or libc6)2.18 and earlier allows context-dependent service (out-of-bounds write and crash) or possibly execute arbitrary code via a crafted (1) NTFS or (2) CIFS
CVE-2015-8778	glibc-2.17-292.el7.x86_64	glibc	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23allows context-dependent attackers to c (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, whic heap-memory access.
CVE-2015-8778	glibc-common-2.17-292.el7.x86_64	glibc-common	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23allows context-dependent attackers to c (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, whic heap-memory access.
CVE-2014-7817	glibc-2.17-292.el7.x86_64	glibc	The wordexp function in GNU C Library (aka glibc) 2.21 does notenforce the WRDE_NOCMD flag, which allo attackers to execute arbitrary commands, as demonstrated by input containing "$((`...`))".
CVE-2014-7817	glibc-common-2.17-292.el7.x86_64	glibc-common	The wordexp function in GNU C Library (aka glibc) 2.21 does notenforce the WRDE_NOCMD flag, which allo attackers to execute arbitrary commands, as demonstrated by input containing "$((`...`))".
CVE-2013-2207	glibc-2.17-292.el7.x86_64	glibc	pt_chown in GNU C Library (aka glibc or libc6) before 2.18 does not properly check permissions for tty files, change the permission on the files and obtain access to arbitrary pseudo-terminals by leveraging a FUSE file
CVE-2013-2207	glibc-common-2.17-292.el7.x86_64	glibc-common	pt_chown in GNU C Library (aka glibc or libc6) before 2.18 does not properly check permissions for tty files, change the permission on the files and obtain access to arbitrary pseudo-terminals by leveraging a FUSE file
CVE-2013-7345	file-5.11-35.el7.x86_64	file	The BEGIN regular expression in the awk script detector in magic/Magdir/commands in file before 5.15 uses unlimited repetitions, which allows context-dependent attackers to cause a denial of service (CPU consumpti triggers a large amount of backtracking, as demonstrated via a file with many newline characters.
CVE-2013-7345	file-libs-5.11-35.el7.x86_64	file-libs	The BEGIN regular expression in the awk script detector in magic/Magdir/commands in file before 5.15 uses unlimited repetitions, which allows context-dependent attackers to cause a denial of service (CPU consumpti triggers a large amount of backtracking, as demonstrated via a file with many newline characters.
CVE-2018-6485	glibc-2.17-292.el7.x86_64	glibc	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to h
CVE-2018-6485	glibc-common-2.17-292.el7.x86_64	glibc-common	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to h
CVE-2017-1213	glibc-2.17-292.el7.x86_64	glibc	• • This candidate has been reserved by an organization or individual that will use it when announcing a n candidate has been publicized, the details for this candidate will be provided.
CVE-2017-1213	glibc-common-2.17-292.el7.x86_64	glibc-common	• • This candidate has been reserved by an organization or individual that will use it when announcing a n candidate has been publicized, the details for this candidate will be provided.
CVE-2015-1472	glibc-2.17-292.el7.x86_64	glibc	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not p during memory allocation, which allows context-dependent attackers to cause a denial of service (buffer over unspecified other impact via a long line containing wide characters that are improperly handled in a wscanf c
CVE-2015-1472	glibc-common-2.17-292.el7.x86_64	glibc-common	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not p during memory allocation, which allows context-dependent attackers to cause a denial of service (buffer over unspecified other impact via a long line containing wide characters that are improperly handled in a wscanf c
CVE-2014-9652	file-5.11-35.el7.x86_64	file	The mconvert function in softmagic.c in file before 5.21, as used in the Fileinfo component in PHP before 5.4 5.6.x before 5.6.5, does not properly handle a certain string-length field during a copy of a truncated version allow remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via
CVE-2014-9652	file-libs-5.11-35.el7.x86_64	file-libs	The mconvert function in softmagic.c in file before 5.21, as used in the Fileinfo component in PHP before 5.4 5.6.x before 5.6.5, does not properly handle a certain string-length field during a copy of a truncated version allow remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via
CVE-2015-5180	glibc-2.17-292.el7.x86_64	glibc	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer crash).
CVE-2015-5180	glibc-common-2.17-292.el7.x86_64	glibc-common	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer crash).
CVE-2014-0475	glibc-2.17-292.el7.x86_64	glibc	Multiple directory traversal vulnerabilities in GNU C Library (akaglibc or libc6) before 2.20 allow context-depe ForceCommand restrictions and possibly have other unspecified impact via a .. (dot dot) in a (1) LC_*, (2) LA environment variable.

CVE-2014-0475	glibc-common-2.17-292.el7.x86_64	glibc-common	Multiple directory traversal vulnerabilities in GNU C Library (akaglibc or libc6) before 2.20 allow context-depe ForceCommand restrictions and possibly have other unspecified impact via a .. (dot dot) in a (1) LC_*, (2) LA environment variable.
cve-2010-0001	gzip-1.5-10.el7.x86_64	gzip	Integer underflow in the unlzw function in unlzw.c in gzip before 1.4 on 64-bit platforms, as used in ncompres remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a craf compression, leading to an array index error.
CVE-2018-17199	httpd24-httpd-2.4.34-15.el7.x86_64	httpd24-httpd	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before de causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded w
CVE-2018-17199	httpd24-httpd-tools-2.4.34-15.el7.x86_64	httpd24-httpd-tools	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before de causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded w
CVE-2018-17199	httpd24-mod_session-2.4.34-15.el7.x86_64	httpd24-mod_session	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before de causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded w
CVE-2018-17199	httpd24-mod_ssl-2.4.34-15.el7.x86_64	httpd24-mod_ssl	In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before de causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded w
CVE-2018-17189	httpd24-httpd-2.4.34-15.el7.x86_64	httpd24-httpd	In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resc request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (m
CVE-2018-17189	httpd24-httpd-tools-2.4.34-15.el7.x86_64	httpd24-httpd-tools	In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resc request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (m
CVE-2018-17189	httpd24-mod_session-2.4.34-15.el7.x86_64	httpd24-mod_session	In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resc request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (m
CVE-2018-17189	httpd24-mod_ssl-2.4.34-15.el7.x86_64	httpd24-mod_ssl	In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resc request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (m
CVE-2019-10092	httpd24-httpd-2.4.34-15.el7.x86_64	httpd24-httpd	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_pro cause the link on the error page to be malformed and instead point to a page of their choice. This would only was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displa
CVE-2019-10092	httpd24-httpd-tools-2.4.34-15.el7.x86_64	httpd24-httpd-tools	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_pro cause the link on the error page to be malformed and instead point to a page of their choice. This would only was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displa
CVE-2019-10092	httpd24-mod_session-2.4.34-15.el7.x86_64	httpd24-mod_session	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_pro cause the link on the error page to be malformed and instead point to a page of their choice. This would only was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displa
CVE-2019-10092	httpd24-mod_ssl-2.4.34-15.el7.x86_64	httpd24-mod_ssl	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_pro cause the link on the error page to be malformed and instead point to a page of their choice. This would only was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displa
CVE-2019-9517	httpd24-httpd-2.4.34-15.el7.x86_64	httpd24-httpd	Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window clo write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response obje servers queue the responses, this can consume excess memory, CPU, or both.
CVE-2019-9517	httpd24-httpd-tools-2.4.34-15.el7.x86_64	httpd24-httpd-tools	Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window clo write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response obje servers queue the responses, this can consume excess memory, CPU, or both.
CVE-2019-9517	httpd24-mod_session-2.4.34-15.el7.x86_64	httpd24-mod_session	Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window clo write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response obje servers queue the responses, this can consume excess memory, CPU, or both.
CVE-2019-9517	httpd24-mod_ssl-2.4.34-15.el7.x86_64	httpd24-mod_ssl	Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window clo write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response obje servers queue the responses, this can consume excess memory, CPU, or both.
CVE-2019-0217	httpd24-httpd-2.4.34-15.el7.x86_64	httpd24-httpd	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a user with valid credentials to authenticate using another username, bypassing configured access control rest
CVE-2019-0217	httpd24-httpd-tools-2.4.34-15.el7.x86_64	httpd24-httpd-tools	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a user with valid credentials to authenticate using another username, bypassing configured access control rest
CVE-2019-0217	httpd24-mod_session-2.4.34-15.el7.x86_64	httpd24-mod_session	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a user with valid credentials to authenticate using another username, bypassing configured access control rest
CVE-2019-0217	httpd24-mod_ssl-2.4.34-15.el7.x86_64	httpd24-mod_ssl	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a user with valid credentials to authenticate using another username, bypassing configured access control rest
CVE-2019-9516	httpd24-httpd-2.4.34-15.el7.x86_64	httpd24-httpd	Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. The headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or implementations allocate memory for these headers and keep the allocation alive until the session dies. This
CVE-2019-9516	httpd24-httpd-tools-2.4.34-15.el7.x86_64	httpd24-httpd-tools	Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. The headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or implementations allocate memory for these headers and keep the allocation alive until the session dies. This

CVE-2019-9516	httpd24-mod_session-2.4.34-15.el7.x86_64	httpd24-mod_session	Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. Th headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or implementations allocate memory for these headers and keep the allocation alive until the session dies. This
CVE-2019-9516	httpd24-mod_ssl-2.4.34-15.el7.x86_64	httpd24-mod_ssl	Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. Th headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or implementations allocate memory for these headers and keep the allocation alive until the session dies. This
CVE-2019-9511	httpd24-httpd-2.4.34-15.el7.x86_64	httpd24-httpd	Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipul denial of service. The attacker requests a large amount of data from a specified resource over multiple strea size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently consume excess CPU, memory, or both.
CVE-2019-9511	httpd24-httpd-tools-2.4.34-15.el7.x86_64	httpd24-httpd-tools	Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipul denial of service. The attacker requests a large amount of data from a specified resource over multiple strea size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently consume excess CPU, memory, or both.
CVE-2019-9511	httpd24-libnghttp2-1.7.1-8.el7.x86_64	httpd24-libnghttp2	Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipul denial of service. The attacker requests a large amount of data from a specified resource over multiple strea size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently consume excess CPU, memory, or both.
CVE-2019-9511	httpd24-mod_session-2.4.34-15.el7.x86_64	httpd24-mod_session	Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipul denial of service. The attacker requests a large amount of data from a specified resource over multiple strea size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently consume excess CPU, memory, or both.
CVE-2019-9511	httpd24-mod_ssl-2.4.34-15.el7.x86_64	httpd24-mod_ssl	Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipul denial of service. The attacker requests a large amount of data from a specified resource over multiple strea size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently consume excess CPU, memory, or both.
CVE-2019-10097	httpd24-httpd-2.4.34-15.el7.x86_64	httpd24-httpd	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary pro protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. triggered by a trusted proxy and not by untrusted HTTP clients.
CVE-2019-10097	httpd24-httpd-tools-2.4.34-15.el7.x86_64	httpd24-httpd-tools	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary pro protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. triggered by a trusted proxy and not by untrusted HTTP clients.
CVE-2019-10097	httpd24-mod_session-2.4.34-15.el7.x86_64	httpd24-mod_session	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary pro protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. triggered by a trusted proxy and not by untrusted HTTP clients.
CVE-2019-10097	httpd24-mod_ssl-2.4.34-15.el7.x86_64	httpd24-mod_ssl	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary pro protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. triggered by a trusted proxy and not by untrusted HTTP clients.
CVE-2019-0220	httpd24-httpd-2.4.34-15.el7.x86_64	httpd24-httpd	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request UR consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in re aspects of the servers processing will implicitly collapse them.
CVE-2019-0220	httpd24-httpd-tools-2.4.34-15.el7.x86_64	httpd24-httpd-tools	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request UR consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in re aspects of the servers processing will implicitly collapse them.
CVE-2019-0220	httpd24-mod_session-2.4.34-15.el7.x86_64	httpd24-mod_session	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request UR consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in re aspects of the servers processing will implicitly collapse them.
CVE-2019-0220	httpd24-mod_ssl-2.4.34-15.el7.x86_64	httpd24-mod_ssl	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request UR consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in re aspects of the servers processing will implicitly collapse them.
CVE-2019-9513	httpd24-libnghttp2-1.7.1-8.el7.x86_64	httpd24-libnghttp2	Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service. TH request streams and continually shuffles the priority of the streams in a way that causes substantial churn to consume excess CPU.
CVE-2012-1088	iproute-4.11.0-25.el7.x86_64	iproute	iproute2 before 3.3.0 allows local users to overwrite arbitrary files via a symlink attack on a temporary file use examples/dhcp-client-script.
CVE-2014-8964	pcre-8.32-17.el7.x86_64	pcre	Heap-based buffer overflow in PCRE 8.36 and earlier allows remote attackers to cause a denial of service (c impact via a crafted regular expression, related to an assertion that allows zero repeats.
CVE-2010-4180	openssl-1.0.2k-19.el7.x86_64	openssl	OpenSSL before 0.9.8q, and 1.0.x before 1.0.0c, when SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_ properly prevent modification of the ciphersuite in the session cache, which allows remote attackers to force unintended cipher via vectors involving sniffing network traffic to discover a session identifier.
CVE-2018-0735	openssl-1.0.2k-19.el7.x86_64	openssl	The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). (Affected 1.1.1).
CVE-2018-0739	openssl-1.0.2k-19.el7.x86_64	openssl	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exce input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures u from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in 1.0.2b-1.0.2n).
CVE-2018-5407	openssl-1.0.2k-19.el7.x86_64	openssl	Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to tir timing attack on 'port contention'.

CVE-2017-3737	openssl-1.0.2k-19.el7.x86_64	openssl	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to cor works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_conn does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. I application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected
CVE-2017-3735	openssl-1.0.2k-19.el7.x86_64	openssl	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of 1.1.0g.
CVE-2018-0734	openssl-1.0.2k-19.el7.x86_64	openssl	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSI Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).
CVE-2018-0495	openssl-1.0.2k-19.el7.x86_64	openssl	Libgcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signat through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ec Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the loc machine on the same physical host.
CVE-2018-0732	openssl-1.0.2k-19.el7.x86_64	openssl	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a v client. This will cause the client to spend an unreasonably long period of time generating a key for this prime client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affec OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).
CVE-2018-0737	openssl-1.0.2k-19.el7.x86_64	openssl	The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side chann sufficient access to mount cache timing attacks during the RSA key generation process could recover the pri 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).
CVE-2017-3736	openssl-1.0.2k-19.el7.x86_64	openssl	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most deduce information about a private key may be performed offline. The amount of resources required for such significant and likely only accessible to a limited number of attackers. An attacker would additionally need on system using the target private key in a scenario with persistent DH parameters and a private key that is sha This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th gener
CVE-2017-3738	openssl-1.0.2k-19.el7.x86_64	openssl	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024 are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very dif believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to private key may be performed offline. The amount of resources required for such an attack would be significa TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswe impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e5(repository.
CVE-2017-17807	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The KEYS subsystem in the Linux kernel before 4.14.6 omitted an access-control check when adding a key t request-key keyring" via the request_key() system call, allowing a local user to use a sequence of crafted sys keyring with only Search permission (not Write permission) to that keyring, related to construct_get_dest_key security/keys/request_key.c.
CVE-2017-17807	perf-3.10.0-1127.13.1.el7.x86_64	perf	The KEYS subsystem in the Linux kernel before 4.14.6 omitted an access-control check when adding a key t request-key keyring" via the request_key() system call, allowing a local user to use a sequence of crafted sys keyring with only Search permission (not Write permission) to that keyring, related to construct_get_dest_key security/keys/request_key.c.
CVE-2019-3819	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the Linux kernel in the function hid_debug_events_read() in drivers/hid/hid-debug.c file w with certain parameters passed from a userspace. A local privileged user ("root") can cause a system lock up Versions from v4.18 and newer are vulnerable.
CVE-2019-3819	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the Linux kernel in the function hid_debug_events_read() in drivers/hid/hid-debug.c file w with certain parameters passed from a userspace. A local privileged user ("root") can cause a system lock up Versions from v4.18 and newer are vulnerable.
CVE-2019-7221	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free.
CVE-2019-7221	perf-3.10.0-1127.13.1.el7.x86_64	perf	The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free.
CVE-2016-10200	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to denial of service (use-after-free) by making multiple bind system calls without properly ascertaining whether SOCK_ZAPPED status, related to net/l2tp/l2tp_ip.c and net/l2tp/l2tp_ip6.c.
CVE-2016-10200	perf-3.10.0-1127.13.1.el7.x86_64	perf	Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to denial of service (use-after-free) by making multiple bind system calls without properly ascertaining whether SOCK_ZAPPED status, related to net/l2tp/l2tp_ip.c and net/l2tp/l2tp_ip6.c.
CVE-2017-17053	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The init_new_context function in arch/x86/include/asm/mmu_context.h in the Linux kernel before 4.12.10 doe from LDT table allocation when forking a new process, allowing a local attacker to achieve a use-after-free or other impact by running a specially crafted program. This vulnerability only affected kernels built with CONFI
CVE-2017-17053	perf-3.10.0-1127.13.1.el7.x86_64	perf	The init_new_context function in arch/x86/include/asm/mmu_context.h in the Linux kernel before 4.12.10 doe from LDT table allocation when forking a new process, allowing a local attacker to achieve a use-after-free or other impact by running a specially crafted program. This vulnerability only affected kernels built with CONFI
CVE-2013-4312	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Linux kernel before 4.4.1 allows local users to bypass file-descriptor limits and cause a denial of service sending each descriptor over a UNIX socket before closing it, related to net/unix/af_unix.c and net/unix/garba

CVE-2013-4312	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Linux kernel before 4.4.1 allows local users to bypass file-descriptor limits and cause a denial of service sending each descriptor over a UNIX socket before closing it, related to net/unix/af_unix.c and net/unix/garba
CVE-2017-18208	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause loop) by triggering use of MADVISE_WILLNEED for a DAX mapping.
CVE-2017-18208	perf-3.10.0-1127.13.1.el7.x86_64	perf	The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause loop) by triggering use of MADVISE_WILLNEED for a DAX mapping.
CVE-2016-3156	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which all denial of service (host OS networking outage) by arranging for a large number of IP addresses.
CVE-2016-3156	perf-3.10.0-1127.13.1.el7.x86_64	perf	The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which all denial of service (host OS networking outage) by arranging for a large number of IP addresses.
CVE-2017-7645	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c.
CVE-2017-7645	perf-3.10.0-1127.13.1.el7.x86_64	perf	The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c.
CVE-2016-9685	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Multiple memory leaks in error paths in fs/xfs/xfs_attr_list.c in the Linux kernel before 4.5.1 allow local users (memory consumption) via crafted XFS filesystem operations.
CVE-2016-9685	perf-3.10.0-1127.13.1.el7.x86_64	perf	Multiple memory leaks in error paths in fs/xfs/xfs_attr_list.c in the Linux kernel before 4.5.1 allow local users (memory consumption) via crafted XFS filesystem operations.
CVE-2014-1690	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The help function in net/netfilter/nf_nat_irc.c in the Linux kernel before 3.12.8 allows remote attackers to obta kernel memory by establishing an IRC DCC session in which incorrect packet data is transmitted during use
CVE-2014-1690	perf-3.10.0-1127.13.1.el7.x86_64	perf	The help function in net/netfilter/nf_nat_irc.c in the Linux kernel before 3.12.8 allows remote attackers to obta kernel memory by establishing an IRC DCC session in which incorrect packet data is transmitted during use
CVE-2017-2583	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 imp NULL selector" instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gai crafted application.
CVE-2017-2583	perf-3.10.0-1127.13.1.el7.x86_64	perf	The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 imp NULL selector" instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gai crafted application.
CVE-2018-7757	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Memory leak in the sas_smp_get_phy_events function in drivers/scsi/libsas/sas_expander.c in the Linux kern users to cause a denial of service (memory consumption) via many read accesses to files in the /sys/class/sa demonstrated by the /sys/class/sas_phy/phy-1:0:12/invalid_dword_count file.
CVE-2018-7757	perf-3.10.0-1127.13.1.el7.x86_64	perf	Memory leak in the sas_smp_get_phy_events function in drivers/scsi/libsas/sas_expander.c in the Linux kern users to cause a denial of service (memory consumption) via many read accesses to files in the /sys/class/sa demonstrated by the /sys/class/sas_phy/phy-1:0:12/invalid_dword_count file.
CVE-2018-10883	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write in jbd2_ denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.
CVE-2018-10883	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write in jbd2_ denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.
CVE-2018-13093	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in fs/xfs/xfs_icache.c in the Linux kernel through 4.17.3. There is a NULL pointer de lookup_slow() on a NULL inode->i_ops pointer when doing pathwalks on a corrupted xfs image. This occurs validation that cached inodes are free during allocation.
CVE-2018-13093	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in fs/xfs/xfs_icache.c in the Linux kernel through 4.17.3. There is a NULL pointer de lookup_slow() on a NULL inode->i_ops pointer when doing pathwalks on a corrupted xfs image. This occurs validation that cached inodes are free during allocation.
CVE-2017-15649	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	net/packet/af_packet.c in the Linux kernel before 4.13.6 allows local users to gain privileges via crafted syste of packet_fanout data structures, because of a race condition (involving fanout_add and packet_do_bind) tha different vulnerability than CVE-2017-6346.
CVE-2017-15649	perf-3.10.0-1127.13.1.el7.x86_64	perf	net/packet/af_packet.c in the Linux kernel before 4.13.6 allows local users to gain privileges via crafted syste of packet_fanout data structures, because of a race condition (involving fanout_add and packet_do_bind) tha different vulnerability than CVE-2017-6346.
CVE-2016-8655	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileg (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packe packet_setsockopt functions.
CVE-2016-8655	perf-3.10.0-1127.13.1.el7.x86_64	perf	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileg (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packe packet_setsockopt functions.
CVE-2016-2117	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The atl2_probe function in drivers/net/ethernet/atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly which allows remote attackers to obtain sensitive information from kernel memory by reading packet data.
CVE-2016-2117	perf-3.10.0-1127.13.1.el7.x86_64	perf	The atl2_probe function in drivers/net/ethernet/atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly which allows remote attackers to obtain sensitive information from kernel memory by reading packet data.
CVE-2016-8630	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The x86_decode_insn function in arch/x86/kvm/emulate.c in the Linux kernel before 4.8.7, when KVM is ena cause a denial of service (host OS crash) via a certain use of a ModR/M byte in an undefined instruction.

CVE-2016-8630	perf-3.10.0-1127.13.1.el7.x86_64	perf	The x86_decode_insn function in arch/x86/kvm/emulate.c in the Linux kernel before 4.8.7, when KVM is ena cause a denial of service (host OS crash) via a certain use of a ModR/M byte in an undefined instruction.
CVE-2017-17558	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The usb_destroy_configuration function in drivers/usb/core/config.c in the USB core subsystem in the Linux l consider the maximum number of configurations and interfaces before attempting to release resources, whic denial of service (out-of-bounds write access) or possibly have unspecified other impact via a crafted USB de
CVE-2017-17558	perf-3.10.0-1127.13.1.el7.x86_64	perf	The usb_destroy_configuration function in drivers/usb/core/config.c in the USB core subsystem in the Linux l consider the maximum number of configurations and interfaces before attempting to release resources, whic denial of service (out-of-bounds write access) or possibly have unspecified other impact via a crafted USB de
CVE-2016-8645	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The TCP stack in the Linux kernel before 4.8.10 mishandles skb truncation, which allows local users to caus crash) via a crafted application that makes sendto system calls, related to net/ipv4/tcp_ipv4.c and net/ipv6/tc
CVE-2016-8645	perf-3.10.0-1127.13.1.el7.x86_64	perf	The TCP stack in the Linux kernel before 4.8.10 mishandles skb truncation, which allows local users to caus crash) via a crafted application that makes sendto system calls, related to net/ipv4/tcp_ipv4.c and net/ipv6/tc
CVE-2017-9725	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In all Qualcomm products with Android releases from CAF using the Linux kernel, during DMA allocation, du allocation size gets truncated which makes allocation succeed when it should fail.
CVE-2017-9725	perf-3.10.0-1127.13.1.el7.x86_64	perf	In all Qualcomm products with Android releases from CAF using the Linux kernel, during DMA allocation, du allocation size gets truncated which makes allocation succeed when it should fail.
CVE-2016-2847	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	fs/pipe.c in the Linux kernel before 4.5 does not limit the amount of unread data in pipes, which allows local u service (memory consumption) by creating many pipes with non-default sizes.
CVE-2016-2847	perf-3.10.0-1127.13.1.el7.x86_64	perf	fs/pipe.c in the Linux kernel before 4.5 does not limit the amount of unread data in pipes, which allows local u service (memory consumption) by creating many pipes with non-default sizes.
CVE-2018-10853	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the way Linux kernel KVM hypervisor before 4.18 emulated instructions such as sgdt/sid current privilege(CPL) level while emulating unprivileged instructions. An unprivileged guest user/process co escalate privileges inside guest.
CVE-2018-10853	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the way Linux kernel KVM hypervisor before 4.18 emulated instructions such as sgdt/sid current privilege(CPL) level while emulating unprivileged instructions. An unprivileged guest user/process co escalate privileges inside guest.
CVE-2019-11487	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Linux kernel before 5.1-rc5 allows page->_refcount reference count overflow, with resultant use-after-fre 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 mm/gup.c, and mm/hugetlb.c. It can occur with FUSE requests.
CVE-2019-11487	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Linux kernel before 5.1-rc5 allows page->_refcount reference count overflow, with resultant use-after-fre 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 mm/gup.c, and mm/hugetlb.c. It can occur with FUSE requests.
CVE-2019-17666	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel through 5.3.6 lacks a certain uppe buffer overflow.
CVE-2019-17666	perf-3.10.0-1127.13.1.el7.x86_64	perf	rtl_p2p_noa_ie in drivers/net/wireless/realtek/rtlwifi/ps.c in the Linux kernel through 5.3.6 lacks a certain uppe buffer overflow.
CVE-2017-2618	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the Linux kernel's handling of clearing SELinux attributes on /proc/pid/attr files before 4.9 this file can crash the system by causing the system to attempt to access unmapped kernel memory.
CVE-2017-2618	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the Linux kernel's handling of clearing SELinux attributes on /proc/pid/attr files before 4.9 this file can crash the system by causing the system to attempt to access unmapped kernel memory.
CVE-2020-12888	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The VFIO PCI driver in the Linux kernel through 5.6.13 mishandles attempts to access disabled memory spa
CVE-2020-12888	perf-3.10.0-1127.13.1.el7.x86_64	perf	The VFIO PCI driver in the Linux kernel through 5.6.13 mishandles attempts to access disabled memory spa
CVE-2015-4700	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The bpf_int_jit_compile function in arch/x86/net/bpf_jit_comp.c in the Linux kernel before 4.0.6 allows local u service (system crash) by creating a packet filter and then loading crafted BPF instructions that trigger late c
CVE-2015-4700	perf-3.10.0-1127.13.1.el7.x86_64	perf	The bpf_int_jit_compile function in arch/x86/net/bpf_jit_comp.c in the Linux kernel before 4.0.6 allows local u service (system crash) by creating a packet filter and then loading crafted BPF instructions that trigger late c
CVE-2019-6974	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference cou condition, leading to a use-after-free.
CVE-2019-6974	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference cou condition, leading to a use-after-free.
CVE-2017-15129	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A use-after-free vulnerability was found in network namespaces code affecting the Linux kernel before 4.14.1 get_net_ns_by_id() in net/core/net_namespace.c does not check for the net::count value after it has found a which could lead to double free and memory corruption. This vulnerability could allow an unprivileged local u corruption on the system, leading to a crash. Due to the nature of the flaw, privilege escalation cannot be full thought to be unlikely.
CVE-2017-15129	perf-3.10.0-1127.13.1.el7.x86_64	perf	A use-after-free vulnerability was found in network namespaces code affecting the Linux kernel before 4.14.1 get_net_ns_by_id() in net/core/net_namespace.c does not check for the net::count value after it has found a which could lead to double free and memory corruption. This vulnerability could allow an unprivileged local u corruption on the system, leading to a crash. Due to the nature of the flaw, privilege escalation cannot be full thought to be unlikely.
CVE-2017-17449	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The __netlink_deliver_tap_skb function in net/netlink/af_netlink.c in the Linux kernel through 4.14.4, when C does not restrict observations of Netlink messages to a single net namespace, which allows local users to ob leveraging the CAP_NET_ADMIN capability to sniff an nlmon interface for all Netlink activity on the system.

CVE-2017-17449	perf-3.10.0-1127.13.1.el7.x86_64	perf	The __netlink_deliver_tap_skb function in net/netlink/af_netlink.c in the Linux kernel through 4.14.4, when C does not restrict observations of Netlink messages to a single net namespace, which allows local users to ob leveraging the CAP_NET_ADMIN capability to sniff an nlmon interface for all Netlink activity on the system.
CVE-2017-16939	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows loca cause a denial of service (use-after-free) via a crafted SO_RCVBUF setsockopt system call in conjunction wi Netlink messages.
CVE-2017-16939	perf-3.10.0-1127.13.1.el7.x86_64	perf	The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows loca cause a denial of service (use-after-free) via a crafted SO_RCVBUF setsockopt system call in conjunction wi Netlink messages.
CVE-2014-6416	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Buffer overflow in net/ceph/auth_x.c in Ceph, as used in the Linux kernel before 3.16.3, allows remote attack (memory corruption and panic) or possibly have unspecified other impact via a long unencrypted auth ticket.
CVE-2014-6416	perf-3.10.0-1127.13.1.el7.x86_64	perf	Buffer overflow in net/ceph/auth_x.c in Ceph, as used in the Linux kernel before 3.16.3, allows remote attack (memory corruption and panic) or possibly have unspecified other impact via a long unencrypted auth ticket.
CVE-2014-8171	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The memory resource controller (aka memcg) in the Linux kernel allows local users to cause a denial of serv new processes within a memory-constrained cgroup.
CVE-2014-8171	perf-3.10.0-1127.13.1.el7.x86_64	perf	The memory resource controller (aka memcg) in the Linux kernel allows local users to cause a denial of serv new processes within a memory-constrained cgroup.
CVE-2017-14140	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The move_pages system call in mm/migrate.c in the Linux kernel before 4.12.9 doesn't check the effective u enabling a local attacker to learn the memory layout of a setuid executable despite ASLR.
CVE-2017-14140	perf-3.10.0-1127.13.1.el7.x86_64	perf	The move_pages system call in mm/migrate.c in the Linux kernel before 4.12.9 doesn't check the effective u enabling a local attacker to learn the memory layout of a setuid executable despite ASLR.
CVE-2013-4587	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Array index error in the kvm_vm_ioctl_create_vcpu function in virt/kvm/kvm_main.c in the KVM subsystem in 3.12.5 allows local users to gain privileges via a large id value.
CVE-2013-4587	perf-3.10.0-1127.13.1.el7.x86_64	perf	Array index error in the kvm_vm_ioctl_create_vcpu function in virt/kvm/kvm_main.c in the KVM subsystem in 3.12.5 allows local users to gain privileges via a large id value.
CVE-2016-3070	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The trace_writeback_dirty_page implementation in include/trace/events/writeback.h in the Linux kernel befor mm/migrate.c, which allows local users to cause a denial of service (NULL pointer dereference and system c unspecified other impact by triggering a certain page move.
CVE-2016-3070	perf-3.10.0-1127.13.1.el7.x86_64	perf	The trace_writeback_dirty_page implementation in include/trace/events/writeback.h in the Linux kernel befor mm/migrate.c, which allows local users to cause a denial of service (NULL pointer dereference and system c unspecified other impact by triggering a certain page move.
CVE-2016-6213	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	fs/namespace.c in the Linux kernel before 4.9 does not restrict how many mounts may exist in a mount name users to cause a denial of service (memory consumption and deadlock) via MS_BIND mount system calls, a triggers exponential growth in the number of mounts.
CVE-2016-6213	perf-3.10.0-1127.13.1.el7.x86_64	perf	fs/namespace.c in the Linux kernel before 4.9 does not restrict how many mounts may exist in a mount name users to cause a denial of service (memory consumption and deadlock) via MS_BIND mount system calls, a triggers exponential growth in the number of mounts.
CVE-2015-2666	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Stack-based buffer overflow in the get_matching_model_microcode function in arch/x86/kernel/cpu/micrococ kernel before 4.0 allows context-dependent attackers to gain privileges by constructing a crafted microcode h privileges for write access to the initrd.
CVE-2015-2666	perf-3.10.0-1127.13.1.el7.x86_64	perf	Stack-based buffer overflow in the get_matching_model_microcode function in arch/x86/kernel/cpu/micrococ kernel before 4.0 allows context-dependent attackers to gain privileges by constructing a crafted microcode h privileges for write access to the initrd.
CVE-2018-20856	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 4.18.7. In block/blk-core.c, there is an __blk_drain_queue certain error case is mishandled.
CVE-2018-20856	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 4.18.7. In block/blk-core.c, there is an __blk_drain_queue certain error case is mishandled.
CVE-2019-10126	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	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.
CVE-2019-10126	perf-3.10.0-1127.13.1.el7.x86_64	perf	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.
CVE-2014-9715	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	include/net/netfilter/nf_conntrack_extend.h in the netfilter subsystem in the Linux kernel before 3.14.5 uses a for certain extension data, which allows local users to cause a denial of service (NULL pointer dereference a network traffic that triggers extension loading, as demonstrated by configuring a PPTP tunnel in a NAT envir
CVE-2014-9715	perf-3.10.0-1127.13.1.el7.x86_64	perf	include/net/netfilter/nf_conntrack_extend.h in the netfilter subsystem in the Linux kernel before 3.14.5 uses a for certain extension data, which allows local users to cause a denial of service (NULL pointer dereference a network traffic that triggers extension loading, as demonstrated by configuring a PPTP tunnel in a NAT envir
CVE-2016-3713	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The msr_mtrr_valid function in arch/x86/kvm/mtrr.c in the Linux kernel before 4.6.1 supports MSR 0x2f8, whi read or write to the kvm_arch_vcpu data structure, and consequently obtain sensitive information or cause a crash), via a crafted ioctl call.
CVE-2016-3713	perf-3.10.0-1127.13.1.el7.x86_64	perf	The msr_mtrr_valid function in arch/x86/kvm/mtrr.c in the Linux kernel before 4.6.1 supports MSR 0x2f8, whi read or write to the kvm_arch_vcpu data structure, and consequently obtain sensitive information or cause a crash), via a crafted ioctl call.

CVE-2017-6951	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The keyring_search_aux function in security/keys/keyring.c in the Linux kernel through 3.14.79 allows local u service (NULL pointer dereference and OOPS) via a request_key system call for the "dead" type.
CVE-2017-6951	perf-3.10.0-1127.13.1.el7.x86_64	perf	The keyring_search_aux function in security/keys/keyring.c in the Linux kernel through 3.14.79 allows local u service (NULL pointer dereference and OOPS) via a request_key system call for the "dead" type.
CVE-2014-1739	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The media_device_enum_entities function in drivers/media/media-device.c in the Linux kernel before 3.14.6 structure, which allows local users to obtain sensitive information from kernel memory by leveraging /dev/me MEDIA_IOC_ENUM_ENTITIES ioctl call.
CVE-2014-1739	perf-3.10.0-1127.13.1.el7.x86_64	perf	The media_device_enum_entities function in drivers/media/media-device.c in the Linux kernel before 3.14.6 structure, which allows local users to obtain sensitive information from kernel memory by leveraging /dev/me MEDIA_IOC_ENUM_ENTITIES ioctl call.
CVE-2017-6353	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	net/sctp/socket.c in the Linux kernel through 4.10.1 does not properly restrict association peel-off operations which allows local users to cause a denial of service (invalid unlock and double free) via a multithreaded app vulnerability exists because of an incorrect fix for CVE-2017-5986.
CVE-2017-6353	perf-3.10.0-1127.13.1.el7.x86_64	perf	net/sctp/socket.c in the Linux kernel through 4.10.1 does not properly restrict association peel-off operations which allows local users to cause a denial of service (invalid unlock and double free) via a multithreaded app vulnerability exists because of an incorrect fix for CVE-2017-5986.
CVE-2017-2647	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The KEYS subsystem in the Linux kernel before 3.18 allows local users to gain privileges or cause a denial o dereference and system crash) via vectors involving a NULL value for a certain match field, related to the ke in keyring.c.
CVE-2017-2647	perf-3.10.0-1127.13.1.el7.x86_64	perf	The KEYS subsystem in the Linux kernel before 3.18 allows local users to gain privileges or cause a denial o dereference and system crash) via vectors involving a NULL value for a certain match field, related to the ke in keyring.c.
CVE-2019-7308	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	kernel/bpf/verifier.c in the Linux kernel before 4.20.6 performs undesirable out-of-bounds speculation on poir including cases of different branches with different state or limits to sanitize, leading to side-channel attacks.
CVE-2019-7308	perf-3.10.0-1127.13.1.el7.x86_64	perf	kernel/bpf/verifier.c in the Linux kernel before 4.20.6 performs undesirable out-of-bounds speculation on poir including cases of different branches with different state or limits to sanitize, leading to side-channel attacks.
CVE-2018-7740	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The resv_map_release function in mm/hugetlb.c in the Linux kernel through 4.15.7 allows local users to caus a crafted application that makes mmap system calls and has a large pgoff argument to the remap_file_pages
CVE-2018-7740	perf-3.10.0-1127.13.1.el7.x86_64	perf	The resv_map_release function in mm/hugetlb.c in the Linux kernel through 4.15.7 allows local users to caus a crafted application that makes mmap system calls and has a large pgoff argument to the remap_file_pages
CVE-2013-1739	nss-3.44.0-4.el7.x86_64	nss	Mozilla Network Security Services (NSS) before 3.15.2 does not ensure that data structures are initialized be allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors tha
CVE-2013-1739	nss-sysinit-3.44.0-4.el7.x86_64	nss-sysinit	Mozilla Network Security Services (NSS) before 3.15.2 does not ensure that data structures are initialized be allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors tha
CVE-2013-1739	nss-tools-3.44.0-4.el7.x86_64	nss-tools	Mozilla Network Security Services (NSS) before 3.15.2 does not ensure that data structures are initialized be allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors tha
CVE-2016-3119	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	The process_db_args function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote auth denial of service (NULL pointer dereference and daemon crash) via a crafted request to modify a principal.
CVE-2016-3119	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	The process_db_args function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote auth denial of service (NULL pointer dereference and daemon crash) via a crafted request to modify a principal.
CVE-2016-3119	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	The process_db_args function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote auth denial of service (NULL pointer dereference and daemon crash) via a crafted request to modify a principal.
CVE-2016-3119	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	The process_db_args function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote auth denial of service (NULL pointer dereference and daemon crash) via a crafted request to modify a principal.
CVE-2018-5729	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal
CVE-2018-5729	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal
CVE-2018-5729	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal
CVE-2018-5729	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal
CVE-2014-5354	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	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, allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash for a keyless principal, as demonstrated by a kadmin "add_principal -nokey" or "purgekeys -all" command.
CVE-2014-5354	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	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, allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash for a keyless principal, as demonstrated by a kadmin "add_principal -nokey" or "purgekeys -all" command.

CVE-2014-5354	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	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, allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash for a keyless principal, as demonstrated by a kadmin "add_principal -nokey" or "purgekeys -all" command.
CVE-2014-5354	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	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, allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash for a keyless principal, as demonstrated by a kadmin "add_principal -nokey" or "purgekeys -all" command.
CVE-2014-9423	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	The svcauth_gss_accept_sec_context function in lib/rpc/svc_auth_gss.c in MIT Kerberos 5 (aka krb5) 1.11.x 1.12.2, and 1.13.x before 1.13.1 transmits uninitialized interposer data to clients, which allows remote attacke information from process heap memory by sniffing the network for data in a handle field.
CVE-2014-9423	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	The svcauth_gss_accept_sec_context function in lib/rpc/svc_auth_gss.c in MIT Kerberos 5 (aka krb5) 1.11.x 1.12.2, and 1.13.x before 1.13.1 transmits uninitialized interposer data to clients, which allows remote attacke information from process heap memory by sniffing the network for data in a handle field.
CVE-2014-9423	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	The svcauth_gss_accept_sec_context function in lib/rpc/svc_auth_gss.c in MIT Kerberos 5 (aka krb5) 1.11.x 1.12.2, and 1.13.x before 1.13.1 transmits uninitialized interposer data to clients, which allows remote attacke information from process heap memory by sniffing the network for data in a handle field.
CVE-2014-9423	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	The svcauth_gss_accept_sec_context function in lib/rpc/svc_auth_gss.c in MIT Kerberos 5 (aka krb5) 1.11.x 1.12.2, and 1.13.x before 1.13.1 transmits uninitialized interposer data to clients, which allows remote attacke information from process heap memory by sniffing the network for data in a handle field.
CVE-2017-11368	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	In MIT Kerberos 5 (aka krb5) 1.7 and later, an authenticated attacker can cause a KDC assertion failure by s S4U2Proxy requests.
CVE-2017-11368	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	In MIT Kerberos 5 (aka krb5) 1.7 and later, an authenticated attacker can cause a KDC assertion failure by s S4U2Proxy requests.
CVE-2017-11368	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	In MIT Kerberos 5 (aka krb5) 1.7 and later, an authenticated attacker can cause a KDC assertion failure by s S4U2Proxy requests.
CVE-2017-11368	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	In MIT Kerberos 5 (aka krb5) 1.7 and later, an authenticated attacker can cause a KDC assertion failure by s S4U2Proxy requests.
CVE-2018-5730	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos containership check by supplying both a "linkdn" and "containerdn" database argument, or by supplying a DN of a container DN string but is not hierarchically within the container DN.
CVE-2018-5730	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos containership check by supplying both a "linkdn" and "containerdn" database argument, or by supplying a DN of a container DN string but is not hierarchically within the container DN.
CVE-2018-5730	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos containership check by supplying both a "linkdn" and "containerdn" database argument, or by supplying a DN of a container DN string but is not hierarchically within the container DN.
CVE-2018-5730	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos containership check by supplying both a "linkdn" and "containerdn" database argument, or by supplying a DN of a container DN string but is not hierarchically within the container DN.
CVE-2016-3120	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	The validate_as_request function in kdc_util.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka k before 1.14.3, when restrict_anonymous_to_tgt is enabled, uses an incorrect client data structure, which allo to cause a denial of service (NULL pointer dereference and daemon crash) via an S4U2Self request.
CVE-2016-3120	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	The validate_as_request function in kdc_util.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka k before 1.14.3, when restrict_anonymous_to_tgt is enabled, uses an incorrect client data structure, which allo to cause a denial of service (NULL pointer dereference and daemon crash) via an S4U2Self request.
CVE-2016-3120	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	The validate_as_request function in kdc_util.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka k before 1.14.3, when restrict_anonymous_to_tgt is enabled, uses an incorrect client data structure, which allo to cause a denial of service (NULL pointer dereference and daemon crash) via an S4U2Self request.
CVE-2016-3120	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	The validate_as_request function in kdc_util.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka k before 1.14.3, when restrict_anonymous_to_tgt is enabled, uses an incorrect client data structure, which allo to cause a denial of service (NULL pointer dereference and daemon crash) via an S4U2Self request.
CVE-2015-2694	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	The kdcpreauth modules in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.2 do not properly track been validated, which allows remote attackers to bypass an intended preauthentication requirement by provi (2) an arbitrary realm name, related to plugins/preauth/otp/main.c and plugins/preauth/pkinit/pkinit_srv.c.
CVE-2015-2694	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	The kdcpreauth modules in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.2 do not properly track been validated, which allows remote attackers to bypass an intended preauthentication requirement by provi (2) an arbitrary realm name, related to plugins/preauth/otp/main.c and plugins/preauth/pkinit/pkinit_srv.c.
CVE-2015-2694	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	The kdcpreauth modules in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.2 do not properly track been validated, which allows remote attackers to bypass an intended preauthentication requirement by provi (2) an arbitrary realm name, related to plugins/preauth/otp/main.c and plugins/preauth/pkinit/pkinit_srv.c.
CVE-2015-2694	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	The kdcpreauth modules in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.2 do not properly track been validated, which allows remote attackers to bypass an intended preauthentication requirement by provi (2) an arbitrary realm name, related to plugins/preauth/otp/main.c and plugins/preauth/pkinit/pkinit_srv.c.
CVE-2017-7562	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	An authentication bypass flaw was found in the way krb5's certauth interface before 1.16.1 handled the valid remote attacker able to communicate with the KDC could potentially use this flaw to impersonate arbitrary pr erroneous circumstances.

CVE-2017-7562	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	An authentication bypass flaw was found in the way krb5's certauth interface before 1.16.1 handled the valid remote attacker able to communicate with the KDC could potentially use this flaw to impersonate arbitrary pr erroneous circumstances.
CVE-2017-7562	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	An authentication bypass flaw was found in the way krb5's certauth interface before 1.16.1 handled the valid remote attacker able to communicate with the KDC could potentially use this flaw to impersonate arbitrary pr erroneous circumstances.
CVE-2017-7562	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	An authentication bypass flaw was found in the way krb5's certauth interface before 1.16.1 handled the valid remote attacker able to communicate with the KDC could potentially use this flaw to impersonate arbitrary pr erroneous circumstances.
CVE-2015-8630	krb5-devel-1.15.1-37.el7_6.x86_64	krb5-devel	The (1) kadm5_create_principal_3 and (2) kadm5_modify_principal functions in lib/kadm5/srv/svr_principal.c (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 caus pointer dereference and daemon crash) by specifying KADM5_POLICY with a NULL policy name.
CVE-2015-8630	krb5-libs-1.15.1-37.el7_6.x86_64	krb5-libs	The (1) kadm5_create_principal_3 and (2) kadm5_modify_principal functions in lib/kadm5/srv/svr_principal.c (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 caus pointer dereference and daemon crash) by specifying KADM5_POLICY with a NULL policy name.
CVE-2015-8630	krb5-workstation-1.15.1-37.el7_6.x86_64	krb5-workstation	The (1) kadm5_create_principal_3 and (2) kadm5_modify_principal functions in lib/kadm5/srv/svr_principal.c (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 caus pointer dereference and daemon crash) by specifying KADM5_POLICY with a NULL policy name.
CVE-2015-8630	libkadm5-1.15.1-37.el7_6.x86_64	libkadm5	The (1) kadm5_create_principal_3 and (2) kadm5_modify_principal functions in lib/kadm5/srv/svr_principal.c (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 caus pointer dereference and daemon crash) by specifying KADM5_POLICY with a NULL policy name.
CVE-2018-14348	libcgroup-0.41-21.el7.x86_64	libcgroup	libcgroup up to and including 0.41 creates /var/log/cgred with mode 0666 regardless of the configured umask information.
CVE-2014-5044	libgcc-4.8.5-39.el7.x86_64	libgcc	Multiple integer overflows in libgfortran might allow remote attackers to execute arbitrary code or cause a der application crash) via vectors related to array allocation.
CVE-2014-5044	libgomp-4.8.5-39.el7.x86_64	libgomp	Multiple integer overflows in libgfortran might allow remote attackers to execute arbitrary code or cause a der application crash) via vectors related to array allocation.
CVE-2014-5044	libstdc++-4.8.5-39.el7.x86_64	libstdc++	Multiple integer overflows in libgfortran might allow remote attackers to execute arbitrary code or cause a der application crash) via vectors related to array allocation.
CVE-2017-11671	libgcc-4.8.5-39.el7.x86_64	libgcc	Under certain circumstances, the ix86_expand_builtin function in i386.c in GNU Compiler Collection (GCC) v before 5.5, and 6 before 6.4 will generate instruction sequences that clobber the status flag of the RDRAND can be read, potentially causing failures of these instructions to go unreported. This could potentially lead to number generation.
CVE-2017-11671	libgomp-4.8.5-39.el7.x86_64	libgomp	Under certain circumstances, the ix86_expand_builtin function in i386.c in GNU Compiler Collection (GCC) v before 5.5, and 6 before 6.4 will generate instruction sequences that clobber the status flag of the RDRAND can be read, potentially causing failures of these instructions to go unreported. This could potentially lead to number generation.
CVE-2017-11671	libstdc++-4.8.5-39.el7.x86_64	libstdc++	Under certain circumstances, the ix86_expand_builtin function in i386.c in GNU Compiler Collection (GCC) v before 5.5, and 6 before 6.4 will generate instruction sequences that clobber the status flag of the RDRAND can be read, potentially causing failures of these instructions to go unreported. This could potentially lead to number generation.
CVE-2015-5276	libgcc-4.8.5-39.el7.x86_64	libgcc	The std::random_device class in libstdc++ in the GNU Compiler Collection (aka GCC) before 4.9.4 does not from blocking sources, which makes it easier for context-dependent attackers to predict the random values v
CVE-2015-5276	libgomp-4.8.5-39.el7.x86_64	libgomp	The std::random_device class in libstdc++ in the GNU Compiler Collection (aka GCC) before 4.9.4 does not from blocking sources, which makes it easier for context-dependent attackers to predict the random values v
CVE-2015-5276	libstdc++-4.8.5-39.el7.x86_64	libstdc++	The std::random_device class in libstdc++ in the GNU Compiler Collection (aka GCC) before 4.9.4 does not from blocking sources, which makes it easier for context-dependent attackers to predict the random values v
CVE-2013-2924	libicu-50.2-3.el7.x86_64	libicu	Use-after-free vulnerability in International Components for Unicode (ICU), as used in Google Chrome before products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via
CVE-2018-11213	libjpeg-turbo-1.2.90-8.el7.x86_64	libjpeg-turbo	An issue was discovered in libjpeg 9a. The get_text_gray_row function in rdppm.c allows remote attackers to (Segmentation fault) via a crafted file.
CVE-2018-11813	libjpeg-turbo-1.2.90-8.el7.x86_64	libjpeg-turbo	libjpeg 9c has a large loop because read_pixel in rdtarga.c mishandles EOF.
CVE-2018-14498	libjpeg-turbo-1.2.90-8.el7.x86_64	libjpeg-turbo	get_8bit_row in rdbmp.c in libjpeg-turbo through 1.5.90 and MozJPEG through 3.3.1 allows attackers to caus (heap-based buffer over-read and application crash) via a crafted 8-bit BMP in which one or more of the colo number of palette entries.
CVE-2018-11212	libjpeg-turbo-1.2.90-8.el7.x86_64	libjpeg-turbo	An issue was discovered in libjpeg 9a. The alloc_sarray function in jmemmgr.c allows remote attackers to ca (divide-by-zero error) via a crafted file.
CVE-2018-11214	libjpeg-turbo-1.2.90-8.el7.x86_64	libjpeg-turbo	An issue was discovered in libjpeg 9a. The get_text_rgb_row function in rdppm.c allows remote attackers to (Segmentation fault) via a crafted file.
CVE-2016-3616	libjpeg-turbo-1.2.90-8.el7.x86_64	libjpeg-turbo	The cjpeg utility in libjpeg allows remote attackers to cause a denial of service (NULL pointer dereference an arbitrary code via a crafted file.
CVE-2012-5644	libuser-0.60-9.el7.x86_64	libuser	libuser has information disclosure when moving user's home directory

CVE-2011-3464	libpng-1.5.13-7.el7_2.x86_64	libpng	Off-by-one error in the png_formatted_warning function in pngerror.c in libpng 1.5.4 through 1.5.7 might allov denial of service (application crash) and possibly execute arbitrary code via unspecified vectors, which trigge
CVE-2013-6954	libpng-1.5.13-7.el7_2.x86_64	libpng	The png_do_expand_palette function in libpng before 1.6.8 allows remote attackers to cause a denial of serv and application crash) via (1) a PLTE chunk of zero bytes or (2) a NULL palette, related to pngrtran.c and pn
CVE-2019-3862	libssh2-1.8.0-3.el7.x86_64	libssh2	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQU message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cau data in the client memory.
CVE-2015-1782	libssh2-1.8.0-3.el7.x86_64	libssh2	The kex_agree_methods function in libssh2 before 1.5.0 allows remote servers to cause a denial of service (unspecified impact via crafted length values in an SSH_MSG_KEXINIT packet.
CVE-2019-3858	libssh2-1.8.0-3.el7.x86_64	libssh2	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is r remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in th
CVE-2019-3861	libssh2-1.8.0-3.el7.x86_64	libssh2	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding le packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial client memory.
CVE-2012-5630	libuser-0.60-9.el7.x86_64	libuser	libuser 0.56 and 0.57 has a TOCTOU (time-of-check time-of-use) race condition when copying and removing
CVE-2013-2064	libxcb-1.13-1.el7.x86_64	libxcb	Integer overflow in X.org libxcb 1.9 and earlier allows X servers to trigger allocation of insufficient memory ar related to the read_packet function.
CVE-2018-3639	microcode_ctl-2.1-53.el7.x86_64	microcode_ctl	Systems with microprocessors utilizing speculative execution andspeculative execution of memory reads bef memory writes are known may allow unauthorized disclosure of information to an attacker with local user acc analysis, aka Speculative Store Bypass (SSB), Variant 4.
CVE-2010-4494	libxml2-2.9.1-6.el7_2.3.x86_64	libxml2	Double free vulnerability in libxml2 2.7.8 and other versions, as used in Google Chrome before 8.0.552.215 a remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to
CVE-2010-4494	libxml2-python-2.9.1-6.el7_2.3.x86_64	libxml2-python	Double free vulnerability in libxml2 2.7.8 and other versions, as used in Google Chrome before 8.0.552.215 a remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to
CVE-2013-1740	nss-3.44.0-4.el7.x86_64	nss	The ssl_Do1stHandshake function in sslsecur.c in libssl in Mozilla Network Security Services (NSS) before 3 feature is enabled, allows man-in-the-middle attackers to spoof SSL servers by using an arbitrary X.509 certi traffic.
CVE-2013-1740	nss-softokn-3.44.0-5.el7.x86_64	nss-softokn	The ssl_Do1stHandshake function in sslsecur.c in libssl in Mozilla Network Security Services (NSS) before 3 feature is enabled, allows man-in-the-middle attackers to spoof SSL servers by using an arbitrary X.509 certi traffic.
CVE-2013-1740	nss-softokn-freebl-3.44.0-5.el7.x86_64	nss-softokn-freebl	The ssl_Do1stHandshake function in sslsecur.c in libssl in Mozilla Network Security Services (NSS) before 3 feature is enabled, allows man-in-the-middle attackers to spoof SSL servers by using an arbitrary X.509 certi traffic.
CVE-2013-1740	nss-sysinit-3.44.0-4.el7.x86_64	nss-sysinit	The ssl_Do1stHandshake function in sslsecur.c in libssl in Mozilla Network Security Services (NSS) before 3 feature is enabled, allows man-in-the-middle attackers to spoof SSL servers by using an arbitrary X.509 certi traffic.
CVE-2013-1740	nss-tools-3.44.0-4.el7.x86_64	nss-tools	The ssl_Do1stHandshake function in sslsecur.c in libssl in Mozilla Network Security Services (NSS) before 3 feature is enabled, allows man-in-the-middle attackers to spoof SSL servers by using an arbitrary X.509 certi traffic.
CVE-2013-1740	nss-util-3.44.0-3.el7.x86_64	nss-util	The ssl_Do1stHandshake function in sslsecur.c in libssl in Mozilla Network Security Services (NSS) before 3 feature is enabled, allows man-in-the-middle attackers to spoof SSL servers by using an arbitrary X.509 certi traffic.
CVE-2015-4000	nss-3.44.0-4.el7.x86_64	nss	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite isenabled on a server but not on a clier DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by re replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the
CVE-2015-4000	nss-sysinit-3.44.0-4.el7.x86_64	nss-sysinit	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite isenabled on a server but not on a clier DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by re replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the
CVE-2015-4000	nss-tools-3.44.0-4.el7.x86_64	nss-tools	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite isenabled on a server but not on a clier DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by re replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the
CVE-2015-4000	nss-util-3.44.0-3.el7.x86_64	nss-util	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite isenabled on a server but not on a clier DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by re replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the
CVE-2013-1620	nss-3.44.0-4.el7.x86_64	nss	The TLS implementation in Mozilla Network Security Services (NSS) does not properly consider timing side- noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, CVE-2013-0169.
CVE-2013-1620	nss-sysinit-3.44.0-4.el7.x86_64	nss-sysinit	The TLS implementation in Mozilla Network Security Services (NSS) does not properly consider timing side- noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, CVE-2013-0169.
CVE-2013-1620	nss-tools-3.44.0-4.el7.x86_64	nss-tools	The TLS implementation in Mozilla Network Security Services (NSS) does not properly consider timing side- noncompliant MAC check operation during the processing of malformed CBC padding, which allows remote distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, CVE-2013-0169.

CVE-2013-5605	nss-softokn-3.44.0-5.el7.x86_64	nss-softokn	Mozilla Network Security Services (NSS) 3.14 before 3.14.5 and 3.15 before 3.15.3 allows remote attackers possibly have unspecified other impact via invalid handshake packets.
CVE-2013-5605	nss-softokn-freebl-3.44.0-5.el7.x86_64	nss-softokn-freebl	Mozilla Network Security Services (NSS) 3.14 before 3.14.5 and 3.15 before 3.15.3 allows remote attackers possibly have unspecified other impact via invalid handshake packets.
CVE-2017-5462	nss-softokn-3.44.0-5.el7.x86_64	nss-softokn	A flaw in DRBG number generation within the Network Security Services (NSS) library where the internal sta bits over. The NSS library has been updated to fix this issue to address this issue and Firefox ESR 52.1 has 3.28.4. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 5
CVE-2017-5462	nss-softokn-freebl-3.44.0-5.el7.x86_64	nss-softokn-freebl	A flaw in DRBG number generation within the Network Security Services (NSS) library where the internal sta bits over. The NSS library has been updated to fix this issue to address this issue and Firefox ESR 52.1 has 3.28.4. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 5
CVE-2013-1741	nss-softokn-3.44.0-5.el7.x86_64	nss-softokn	Integer overflow in Mozilla Network Security Services (NSS) 3.15 before 3.15.3 allows remote attackers to ca possibly have unspecified other impact via a large size value.
CVE-2013-1741	nss-softokn-freebl-3.44.0-5.el7.x86_64	nss-softokn-freebl	Integer overflow in Mozilla Network Security Services (NSS) 3.15 before 3.15.3 allows remote attackers to ca possibly have unspecified other impact via a large size value.
CVE-2013-5606	nss-softokn-3.44.0-5.el7.x86_64	nss-softokn	The CERT_VerifyCert function in lib/certhigh/certvfy.c in Mozilla Network Security Services (NSS) 3.15 befor unexpected return value for an incompatible key-usage certificate when the CERTVerifyLog argument is vali attackers to bypass intended access restrictions via a crafted certificate.
CVE-2013-5606	nss-softokn-freebl-3.44.0-5.el7.x86_64	nss-softokn-freebl	The CERT_VerifyCert function in lib/certhigh/certvfy.c in Mozilla Network Security Services (NSS) 3.15 befor unexpected return value for an incompatible key-usage certificate when the CERTVerifyLog argument is vali attackers to bypass intended access restrictions via a crafted certificate.
CVE-2017-12172	postgresql-libs-9.2.24-1.el7_5.x86_64	postgresql-libs	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 under a non-root operating system account, and database superusers have effective ability to run arbitrary c PostgreSQL provides a script for starting the database server during system boot. Packages of PostgreSQL provide their own, packager-authored startup implementations. Several implementations use a log file name can replace with a symbolic link. As root, they open(), chmod() and/or chown() this log file name. This often s superuser to escalate to root privileges when root starts the server.
CVE-2013-1899	postgresql-libs-9.2.24-1.el7_5.x86_64	postgresql-libs	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 cause a denial of service (file corruption), and allows remote authenticated users to modify configuration sett code, via a connection request using a database name that begins with a "-" (hyphen).
CVE-2013-1901	postgresql-libs-9.2.24-1.el7_5.x86_64	postgresql-libs	PostgreSQL 9.2.x before 9.2.4 and 9.1.x before 9.1.9 does not properlycheck REPLICATION privileges, whic users to bypass intended backup restrictions by calling the (1) pg_start_backup or (2) pg_stop_backup functi
CVE-2018-10915	postgresql-libs-9.2.24-1.el7_5.x86_64	postgresql-libs	A vulnerability was found in libpq, the default PostgreSQL client library where libpq failed to properly reset its connections. If an affected version of libpq was used with "host" or "hostaddr" connection parameters from u bypass client-side connection security features, obtain access to higher privileged connections or potentially SQL injection, by causing the PQescape() functions to malfunction. Postgresql versions before 10.5, 9.6.10, affected.
CVE-2015-5191	open-vm-tools-10.3.0-2.el7.x86_64	open-vm-tools	VMware Tools prior to 10.0.9 contains multiple file system races in libDeployPkg, related to the use of hard-c Successful exploitation of this issue may result in a local privilege escalation. CVSS:3.0/AV:L/AC:H/PR:L/UI:
CVE-2015-7974	ntp-4.2.6p5-29.el7.centos.x86_64	ntp	NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when auth allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a "skeleton key."
CVE-2015-7974	ntpdate-4.2.6p5-29.el7.centos.x86_64	ntpdate	NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when auth allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a "skeleton key."
CVE-2015-8158	ntp-4.2.6p5-29.el7.centos.x86_64	ntp	The getresponse function in ntpq in NTP versions before 4.2.8p9 and 4.3.x before 4.3.90 allows remote attac service (infinite loop) via crafted packets with incorrect values.
CVE-2015-8158	ntpdate-4.2.6p5-29.el7.centos.x86_64	ntpdate	The getresponse function in ntpq in NTP versions before 4.2.8p9 and 4.3.x before 4.3.90 allows remote attac service (infinite loop) via crafted packets with incorrect values.
CVE-2011-4079	openldap-2.4.44-21.el7_6.x86_64	openldap	Off-by-one error in the UTF8StringNormalize function in OpenLDAP 2.4.26 and earlier allows remote attacke (slapd crash) via a zero-length string that triggers a heap-based buffer overflow, as demonstrated using an e value in an LDIF entry.
CVE-2010-0212	openldap-2.4.44-21.el7_6.x86_64	openldap	OpenLDAP 2.4.22 allows remote attackers to cause a denial of service (crash) via a modrdn call with a zero- which is not properly handled by the smr_normalize function and triggers a NULL pointer dereference in the schema_init.c, as demonstrated using the Codenomicon LDAPv3 test suite.
CVE-2013-4449	openldap-2.4.44-21.el7_6.x86_64	openldap	The rwm overlay in OpenLDAP 2.4.23, 2.4.36, and earlier does not properly count references, which allows r denial of service (slapd crash) by unbinding immediately after a search request, which triggers rwm_conn_de context while it is being used by rwm_op_search.
CVE-2010-0211	openldap-2.4.44-21.el7_6.x86_64	openldap	The slap_modrdn2mods function in modrdn.c in OpenLDAP 2.4.22 does not check the return value of a call which allows remote attackers to cause a denial of service (segmentation fault) and possibly execute arbitrar an RDN string containing invalid UTF-8 sequences, which triggers a free of an invalid, uninitialized pointer in as demonstrated using the Codenomicon LDAPv3 test suite.
CVE-2017-9287	openldap-2.4.44-21.el7_6.x86_64	openldap	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.
CVE-2017-15906	openssh-7.4p1-21.el7.x86_64	openssh	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operation allows attackers to create zero-length files.
CVE-2017-15906	openssh-clients-7.4p1-21.el7.x86_64	openssh-clients	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operation allows attackers to create zero-length files.

CVE-2017-15906	openssh-server-7.4p1-21.el7.x86_64	openssh-server	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operation allows attackers to create zero-length files.
CVE-2014-9278	openssh-7.4p1-21.el7.x86_64	openssh	The OpenSSH server, as used in Fedora and Red Hat Enterprise Linux 7 and when running in a Kerberos en authenticated users to log in as another user when they are listed in the .k5users file of that user, which migh authentication requirements that would force a local login.
CVE-2014-9278	openssh-clients-7.4p1-21.el7.x86_64	openssh-clients	The OpenSSH server, as used in Fedora and Red Hat Enterprise Linux 7 and when running in a Kerberos en authenticated users to log in as another user when they are listed in the .k5users file of that user, which migh authentication requirements that would force a local login.
CVE-2014-9278	openssh-server-7.4p1-21.el7.x86_64	openssh-server	The OpenSSH server, as used in Fedora and Red Hat Enterprise Linux 7 and when running in a Kerberos en authenticated users to log in as another user when they are listed in the .k5users file of that user, which migh authentication requirements that would force a local login.
CVE-2016-0777	openssh-7.4p1-21.el7.x86_64	openssh	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allo sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated b
CVE-2016-0777	openssh-clients-7.4p1-21.el7.x86_64	openssh-clients	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allo sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated b
CVE-2016-0777	openssh-server-7.4p1-21.el7.x86_64	openssh-server	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allo sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated b
CVE-2010-4755	openssh-7.4p1-21.el7.x86_64	openssh	The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and ea and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a deni consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expre requests to an sftp daemon, a different vulnerability than CVE-2010-2632.
CVE-2010-4755	openssh-clients-7.4p1-21.el7.x86_64	openssh-clients	The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and ea and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a deni consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expre requests to an sftp daemon, a different vulnerability than CVE-2010-2632.
CVE-2010-4755	openssh-server-7.4p1-21.el7.x86_64	openssh-server	The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and ea and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a deni consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expre requests to an sftp daemon, a different vulnerability than CVE-2010-2632.
CVE-2016-0778	openssh-7.4p1-21.el7.x86_64	openssh	The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6 certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which all denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many
CVE-2016-0778	openssh-clients-7.4p1-21.el7.x86_64	openssh-clients	The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6 certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which all denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many
CVE-2016-0778	openssh-server-7.4p1-21.el7.x86_64	openssh-server	The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6 certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which all denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many
CVE-2013-7041	pam-1.1.8-22.el7.x86_64	pam	The pam_userdb module for Pam uses a case-insensitive method to compare hashed passwords, which ma guess the password via a brute force attack.
CVE-2014-2583	pam-1.1.8-22.el7.x86_64	pam	Multiple directory traversal vulnerabilities in pam_timestamp.c in the pam_timestamp module for Linux-PAM users to create arbitrary files or possibly bypass authentication via a .. (dot dot) in the (1) PAM_RUSER valu (2) PAM_TTY value to the check_tty function, which is used by the format_timestamp_name function.
CVE-2018-20969	patch-2.7.1-12.el7_7.x86_64	patch	do_ed_script in pch.c in GNU patch through 2.7.6 does not block strings beginning with a ! character. NOTE: CVE-2019-13638, but the ! syntax is specific to ed, and is unrelated to a shell metacharacter.
CVE-2019-1010238	pango-1.42.4-4.el7_7.x86_64	pango	Gnome Pango 1.42 and later is affected by: Buffer Overflow. The impact is: The heap based buffer overflow execution. The component is: function name: pango_log2vis_get_embedding_levels, assignment of nchars a attack vector is: Bug can be used when application pass invalid utf-8 strings to functions like pango_itemize.
CVE-2018-15120	pango-1.42.4-4.el7_7.x86_64	pango	libpango in Pango 1.40.8 through 1.42.3, as used in hexchat and other products, allows remote attackers to (application crash) or possibly have unspecified other impact via crafted text with invalid Unicode sequences
CVE-2010-4651	patch-2.7.1-12.el7_7.x86_64	patch	Directory traversal vulnerability in util.c in GNU patch 2.6.1 and earlier allows user-assisted remote attackers files via a filename that is specified with a .. (dot dot) or full pathname, a related issue to CVE-2010-1679.
CVE-2018-6952	patch-2.7.1-12.el7_7.x86_64	patch	A double free exists in the another_hunk function in pch.c in GNU patch through 2.7.6.
CVE-2016-10713	patch-2.7.1-12.el7_7.x86_64	patch	An issue was discovered in GNU patch before 2.7.6. Out-of-bounds access within pch_write_line() in pch.c c crafted input file.
CVE-2016-3191	pcre-8.32-17.el7.x86_64	pcre	The compile_branch function in pcre_compile.c in PCRE 8.x before 8.39 and pcre2_compile.c in PCRE2 bef containing an (*ACCEPT) substring in conjunction with nested parentheses, which allows remote attackers to cause a denial of service (stack-based buffer overflow) via a crafted regular expression, as demonstrated by encountered by Konqueror, aka ZDI-CAN-3542.

CVE-2015-8388	pcre-8.32-17.el7.x86_64	pcre	PCRE before 8.38 mishandles the /(?=di(?<=(?1))
CVE-2015-8391	pcre-8.32-17.el7.x86_64	pcre	The pcre_compile function in pcre_compile.c in PCRE before 8.38 mishandles certain [: nesting, which allow denial of service (CPU consumption) or possibly have unspecified other impact via a crafted regular expressi JavaScript RegExp object encountered by Konqueror.
CVE-2015-2328	pcre-8.32-17.el7.x86_64	pcre	PCRE before 8.36 mishandles the /((?(R)a
CVE-2015-8386	pcre-8.32-17.el7.x86_64	pcre	PCRE before 8.38 mishandles the interaction of lookbehind assertions and mutually recursive subpatterns, w cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted regular exp JavaScript RegExp object encountered by Konqueror.
CVE-2015-3217	pcre-8.32-17.el7.x86_64	pcre	PCRE 7.8 and 8.32 through 8.37, and PCRE2 10.10 mishandle group empty matches, which might allow ren of service (stack-based buffer overflow) via a crafted regular expression, as demonstrated by /^(?☹?(1) .
CVE-2015-8385	pcre-8.32-17.el7.x86_64	pcre	PCRE before 8.38 mishandles the /(?

CVE-2015-5073	pcre-8.32-17.el7.x86_64	pcre	Heap-based buffer overflow in the find_fixedlength function in pcre_compile.c in PCRE before 8.38 allows re denial of service (crash) or obtain sensitive information from heap memory and possibly bypass the ASLR pr crafted regular expression with an excess closing parenthesis.
CVE-2019-11833	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	fs/ext4/extents.c in the Linux kernel through 5.1.2 does not zero out the unused memory region in the extent local users to obtain sensitive information by reading uninitialized data in the filesystem.
CVE-2019-11833	perf-3.10.0-1127.13.1.el7.x86_64	perf	fs/ext4/extents.c in the Linux kernel through 5.1.2 does not zero out the unused memory region in the extent local users to obtain sensitive information by reading uninitialized data in the filesystem.
CVE-2014-2673	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The arch_dup_task_struct function in the Transactional Memory (TM) implementation in arch/powerpc/kerne before 3.13.7 on the powerpc platform does not properly interact with the clone and fork system calls, which denial of service (Program Check and system crash) via certain instructions that are executed with the proce
CVE-2014-2673	perf-3.10.0-1127.13.1.el7.x86_64	perf	The arch_dup_task_struct function in the Transactional Memory (TM) implementation in arch/powerpc/kerne before 3.13.7 on the powerpc platform does not properly interact with the clone and fork system calls, which denial of service (Program Check and system crash) via certain instructions that are executed with the proce
CVE-2017-18344	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The timer_create syscall implementation in kernel/time/posix-timers.c in the Linux kernel before 4.14.8 doesn sigevent->sigev_notify field, which leads to out-of-bounds access in the show_timer function (called when /pr allows userspace applications to read arbitrary kernel memory (on a kernel built with CONFIG_POSIX_TIME CONFIG_CHECKPOINT_RESTORE).
CVE-2017-18344	perf-3.10.0-1127.13.1.el7.x86_64	perf	The timer_create syscall implementation in kernel/time/posix-timers.c in the Linux kernel before 4.14.8 doesn sigevent->sigev_notify field, which leads to out-of-bounds access in the show_timer function (called when /pr allows userspace applications to read arbitrary kernel memory (on a kernel built with CONFIG_POSIX_TIME CONFIG_CHECKPOINT_RESTORE).
CVE-2018-1087	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	kernel KVM before versions kernel 4.16, kernel 4.16-rc7, kernel 4.17-rc1, kernel 4.17-rc2 and kernel 4.17-rc3 way the Linux kernel's KVM hypervisor handled exceptions delivered after a stack switch operation via Mov S During the stack switch operation, the processor did not deliver interrupts and exceptions, rather they are del after the stack switch is executed. An unprivileged KVM guest user could use this flaw to crash the guest or, privileges in the guest.
CVE-2018-1087	perf-3.10.0-1127.13.1.el7.x86_64	perf	kernel KVM before versions kernel 4.16, kernel 4.16-rc7, kernel 4.17-rc1, kernel 4.17-rc2 and kernel 4.17-rc3 way the Linux kernel's KVM hypervisor handled exceptions delivered after a stack switch operation via Mov S During the stack switch operation, the processor did not deliver interrupts and exceptions, rather they are del after the stack switch is executed. An unprivileged KVM guest user could use this flaw to crash the guest or, privileges in the guest.
CVE-2018-18397	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The userfaultfd implementation in the Linux kernel before 4.19.7 mishandles access control for certain UFFD by allowing local users to write data into holes in a tmpfs file (if the user has read-only access to that file, and related to fs/userfaultfd.c and mm/userfaultfd.c.
CVE-2018-18397	perf-3.10.0-1127.13.1.el7.x86_64	perf	The userfaultfd implementation in the Linux kernel before 4.19.7 mishandles access control for certain UFFD by allowing local users to write data into holes in a tmpfs file (if the user has read-only access to that file, and related to fs/userfaultfd.c and mm/userfaultfd.c.
CVE-2017-7518	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the Linux kernel before version 4.12 in the way the KVM module processed the trap flag emulation of the syscall instruction, which leads to a debug exception(#DB) being raised in the guest stack. A could use this flaw to potentially escalate their privileges inside the guest. Linux guests are not affected by th
CVE-2017-7518	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the Linux kernel before version 4.12 in the way the KVM module processed the trap flag emulation of the syscall instruction, which leads to a debug exception(#DB) being raised in the guest stack. A could use this flaw to potentially escalate their privileges inside the guest. Linux guests are not affected by th
CVE-2013-7269	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The nr_recvmsg function in net/netrom/af_netrom.c in the Linux kernel before 3.12.4 updates a certain length associated data structure has been initialized, which allows local users to obtain sensitive information from k recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2013-7269	perf-3.10.0-1127.13.1.el7.x86_64	perf	The nr_recvmsg function in net/netrom/af_netrom.c in the Linux kernel before 3.12.4 updates a certain length associated data structure has been initialized, which allows local users to obtain sensitive information from k recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2013-6382	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Multiple buffer underflows in the XFS implementation in the Linux kernel through 3.12.1 allow local users to c (memory corruption) or possibly have unspecified other impact by leveraging the CAP_SYS_ADMIN capabili XFS_IOC_ATTRLIST_BY_HANDLE or (2) XFS_IOC_ATTRLIST_BY_HANDLE_32 ioctl call with a crafted le xfs_attrlist_by_handle function in fs/xfs/xfs_ioctl.c and the xfs_compat_attrlist_by_handle function in fs/xfs/xfs
CVE-2013-6382	perf-3.10.0-1127.13.1.el7.x86_64	perf	Multiple buffer underflows in the XFS implementation in the Linux kernel through 3.12.1 allow local users to c (memory corruption) or possibly have unspecified other impact by leveraging the CAP_SYS_ADMIN capabili XFS_IOC_ATTRLIST_BY_HANDLE or (2) XFS_IOC_ATTRLIST_BY_HANDLE_32 ioctl call with a crafted le xfs_attrlist_by_handle function in fs/xfs/xfs_ioctl.c and the xfs_compat_attrlist_by_handle function in fs/xfs/xfs
CVE-2017-17448	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	net/netfilter/nfnetlink_cthelper.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN ca operations, which allows local users to bypass intended access restrictions because the nfnl_cthelper_list da net namespaces.
CVE-2017-17448	perf-3.10.0-1127.13.1.el7.x86_64	perf	net/netfilter/nfnetlink_cthelper.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN ca operations, which allows local users to bypass intended access restrictions because the nfnl_cthelper_list da net namespaces.
CVE-2018-6927	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to caus overflow) or possibly have unspecified other impact by triggering a negative wake or requeue value.
CVE-2018-6927	perf-3.10.0-1127.13.1.el7.x86_64	perf	The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to caus overflow) or possibly have unspecified other impact by triggering a negative wake or requeue value.

CVE-2019-12382	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	• • An issue was discovered in drm_load_edid_firmware in drivers/gpu/drm/drm_edid_load.c in the Linux k an unchecked kstrdup of fwstr, which might allow an attacker to cause a denial of service (NULL pointe crash). NOTE: The vendor disputes this issues as not being a vulnerability because kstrdup() returning and there is no chance for a NULL pointer dereference.
CVE-2019-12382	perf-3.10.0-1127.13.1.el7.x86_64	perf	• • An issue was discovered in drm_load_edid_firmware in drivers/gpu/drm/drm_edid_load.c in the Linux k an unchecked kstrdup of fwstr, which might allow an attacker to cause a denial of service (NULL pointe crash). NOTE: The vendor disputes this issues as not being a vulnerability because kstrdup() returning and there is no chance for a NULL pointer dereference.
CVE-2016-3134	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.
CVE-2016-3134	perf-3.10.0-1127.13.1.el7.x86_64	perf	The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.
CVE-2017-1000407	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Linux Kernel 2.6.32 and later are affected by a denial of service, by flooding the diagnostic port 0x80 an leading to a kernel panic.
CVE-2017-1000407	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Linux Kernel 2.6.32 and later are affected by a denial of service, by flooding the diagnostic port 0x80 an leading to a kernel panic.
CVE-2018-10322	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The xfs_dinode_verify function in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.16.3 allows local service (xfs_ilock_attr_map_shared invalid pointer dereference) via a crafted xfs image.
CVE-2018-10322	perf-3.10.0-1127.13.1.el7.x86_64	perf	The xfs_dinode_verify function in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.16.3 allows local service (xfs_ilock_attr_map_shared invalid pointer dereference) via a crafted xfs image.
CVE-2016-0728	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandle error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use- commands.
CVE-2016-0728	perf-3.10.0-1127.13.1.el7.x86_64	perf	The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandle error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use- commands.
CVE-2017-11600	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	net/xfrm/xfrm_policy.c in the Linux kernel through 4.12.3, when CONFIG_XFRM_MIGRATE is enabled, does xfrm_userpolicy_id is XFRM_POLICY_MAX or less, which allows local users to cause a denial of service (ou have unspecified other impact via an XFRM_MSG_MIGRATE xfrm Netlink message.
CVE-2017-11600	perf-3.10.0-1127.13.1.el7.x86_64	perf	net/xfrm/xfrm_policy.c in the Linux kernel through 4.12.3, when CONFIG_XFRM_MIGRATE is enabled, does xfrm_userpolicy_id is XFRM_POLICY_MAX or less, which allows local users to cause a denial of service (ou have unspecified other impact via an XFRM_MSG_MIGRATE xfrm Netlink message.
CVE-2019-3900	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.
CVE-2019-3900	perf-3.10.0-1127.13.1.el7.x86_64	perf	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.
CVE-2013-2930	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The perf_trace_event_perm function in kernel/trace/trace_event_perf.c in the Linux kernel before 3.12.2 does the perf subsystem, which allows local users to enable function tracing via a crafted application.
CVE-2013-2930	perf-3.10.0-1127.13.1.el7.x86_64	perf	The perf_trace_event_perm function in kernel/trace/trace_event_perf.c in the Linux kernel before 3.12.2 does the perf subsystem, which allows local users to enable function tracing via a crafted application.
CVE-2014-3631	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The assoc_array_gc function in the associative-array implementation in lib/assoc_array.c in the Linux kernel implement garbage collection, which allows local users to cause a denial of service (NULL pointer dereferen possibly have unspecified other impact via multiple "keyctl newring" operations followed by a "keyctl timeout"
CVE-2014-3631	perf-3.10.0-1127.13.1.el7.x86_64	perf	The assoc_array_gc function in the associative-array implementation in lib/assoc_array.c in the Linux kernel implement garbage collection, which allows local users to cause a denial of service (NULL pointer dereferen possibly have unspecified other impact via multiple "keyctl newring" operations followed by a "keyctl timeout"
CVE-2014-3182	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Array index error in the logi_dj_raw_event function in drivers/hid/hid-logitech-dj.c in the Linux kernel before 3 proximate attackers to execute arbitrary code or cause a denial of service (invalid kfree) via a crafted device REPORT_TYPE_NOTIF_DEVICE_UNPAIRED value.
CVE-2014-3182	perf-3.10.0-1127.13.1.el7.x86_64	perf	Array index error in the logi_dj_raw_event function in drivers/hid/hid-logitech-dj.c in the Linux kernel before 3 proximate attackers to execute arbitrary code or cause a denial of service (invalid kfree) via a crafted device REPORT_TYPE_NOTIF_DEVICE_UNPAIRED value.
CVE-2018-18445	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	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 bo out-of-bounds memory accesses because adjust_scalar_min_max_vals in kernel/bpf/verifier.c mishandles 3
CVE-2018-18445	perf-3.10.0-1127.13.1.el7.x86_64	perf	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 bo out-of-bounds memory accesses because adjust_scalar_min_max_vals in kernel/bpf/verifier.c mishandles 3
CVE-2014-4027	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The rd_build_device_space function in drivers/target/target_core_rd.c in the Linux kernel before 3.14 does n data structure, which allows local users to obtain sensitive information from ramdisk_mcp memory by leverag
CVE-2014-4027	perf-3.10.0-1127.13.1.el7.x86_64	perf	The rd_build_device_space function in drivers/target/target_core_rd.c in the Linux kernel before 3.14 does n data structure, which allows local users to obtain sensitive information from ramdisk_mcp memory by leverag

CVE-2019-9503	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Broadcom brcmfmac WiFi driver prior to commit a4176ec356c73a46c07c181c6d04039fafa34a9f is vuln bypass. If the brcmfmac driver receives a firmware event frame from a remote source, the is_wlc_event_fran to be discarded and unprocessed. If the driver receives the firmware event frame from the host, the appropri validation can be bypassed if the bus used is USB (for instance by a wifi dongle). This can allow firmware ev source to be processed. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, una able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-
CVE-2019-9503	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Broadcom brcmfmac WiFi driver prior to commit a4176ec356c73a46c07c181c6d04039fafa34a9f is vuln bypass. If the brcmfmac driver receives a firmware event frame from a remote source, the is_wlc_event_fran to be discarded and unprocessed. If the driver receives the firmware event frame from the host, the appropri validation can be bypassed if the bus used is USB (for instance by a wifi dongle). This can allow firmware ev source to be processed. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, una able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-
CVE-2019-19338	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the fix for CVE-2019-11135, in the Linux upstream kernel versions before 5.5 where, the speculative execution of instructions when a TSX Asynchronous Abort (TAA) error occurs. When a guest is r by the TAA flaw (TAA_NO=0), but is not affected by the MDS issue (MDS_NO=1), the guest was to clear the VERW instruction mechanism. But when the MDS_NO=1 bit was exported to the guests, the guests did not u clear the affected buffers. This issue affects guests running on Cascade Lake CPUs and requires that host h Confidentiality of data is the highest threat associated with this vulnerability.
CVE-2019-19338	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the fix for CVE-2019-11135, in the Linux upstream kernel versions before 5.5 where, the speculative execution of instructions when a TSX Asynchronous Abort (TAA) error occurs. When a guest is r by the TAA flaw (TAA_NO=0), but is not affected by the MDS issue (MDS_NO=1), the guest was to clear the VERW instruction mechanism. But when the MDS_NO=1 bit was exported to the guests, the guests did not u clear the affected buffers. This issue affects guests running on Cascade Lake CPUs and requires that host h Confidentiality of data is the highest threat associated with this vulnerability.
CVE-2017-12188	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	arch/x86/kvm/mmu.c in the Linux kernel through 4.13.5, when nested virtualisation is used, does not properly entries to resolve a guest virtual address, which allows L1 guest OS users to execute arbitrary code on the h service (incorrect index during page walking, and host OS crash), aka an "MMU potential stack buffer overru
CVE-2017-12188	perf-3.10.0-1127.13.1.el7.x86_64	perf	arch/x86/kvm/mmu.c in the Linux kernel through 4.13.5, when nested virtualisation is used, does not properly entries to resolve a guest virtual address, which allows L1 guest OS users to execute arbitrary code on the h service (incorrect index during page walking, and host OS crash), aka an "MMU potential stack buffer overru
CVE-2018-1068	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed write to a limited range of kernel memory.
CVE-2018-1068	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed write to a limited range of kernel memory.
CVE-2019-3459	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel b
CVE-2019-3459	perf-3.10.0-1127.13.1.el7.x86_64	perf	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel b
CVE-2014-0206	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Array index error in the aio_read_events_ring function in fs/aio.c in the Linux kernel through 3.15.1 allows loc information from kernel memory via a large head value.
CVE-2014-0206	perf-3.10.0-1127.13.1.el7.x86_64	perf	Array index error in the aio_read_events_ring function in fs/aio.c in the Linux kernel through 3.15.1 allows loc information from kernel memory via a large head value.
CVE-2016-5828	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc plat state, which allows local users to cause a denial of service (invalid process state or TM Bad Thing exception have unspecified other impact by starting and suspending a transaction before an exec system call.
CVE-2016-5828	perf-3.10.0-1127.13.1.el7.x86_64	perf	The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc plat state, which allows local users to cause a denial of service (invalid process state or TM Bad Thing exception have unspecified other impact by starting and suspending a transaction before an exec system call.
CVE-2018-13094	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occ after xfs_da_shrink_inode() is called with a NULL bp.
CVE-2018-13094	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occ after xfs_da_shrink_inode() is called with a NULL bp.
CVE-2018-14646	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Linux kernel before 4.15-rc8 was found to be vulnerable to a NULL pointer dereference bug in the __net the net/netlink/af_netlink.c file. A local attacker could exploit this when a net namespace with a netnsid is ass and a denial of service.
CVE-2018-14646	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Linux kernel before 4.15-rc8 was found to be vulnerable to a NULL pointer dereference bug in the __net the net/netlink/af_netlink.c file. A local attacker could exploit this when a net namespace with a netnsid is ass and a denial of service.
CVE-2013-7270	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The packet_recvmsg function in net/packet/af_packet.c in the Linux kernel before 3.12.4 updates a certain le an associated data structure has been initialized, which allows local users to obtain sensitive information fror recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2013-7270	perf-3.10.0-1127.13.1.el7.x86_64	perf	The packet_recvmsg function in net/packet/af_packet.c in the Linux kernel before 3.12.4 updates a certain le an associated data structure has been initialized, which allows local users to obtain sensitive information fror recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2016-0758	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via
CVE-2016-0758	perf-3.10.0-1127.13.1.el7.x86_64	perf	Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via
CVE-2017-7184	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not valid XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at Ubuntu 16.10 linux-image-* package 4.8.0.41.52.

CVE-2017-7184	perf-3.10.0-1127.13.1.el7.x86_64	perf	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not valid XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at Ubuntu 16.10 linux-image-* package 4.8.0.41.52.
CVE-2013-6376	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The recalculate_apic_map function in arch/x86/kvm/lapic.c in the KVM subsystem in the Linux kernel through to cause a denial of service (host OS crash) via a crafted ICR write operation in x2apic mode.
CVE-2013-6376	perf-3.10.0-1127.13.1.el7.x86_64	perf	The recalculate_apic_map function in arch/x86/kvm/lapic.c in the KVM subsystem in the Linux kernel through to cause a denial of service (host OS crash) via a crafted ICR write operation in x2apic mode.
CVE-2013-7268	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ipx_recvmsg function in net/ipx/af_ipx.c in the Linux kernel before 3.12.4 updates a certain length value associated data structure has been initialized, which allows local users to obtain sensitive information from k recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2013-7268	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ipx_recvmsg function in net/ipx/af_ipx.c in the Linux kernel before 3.12.4 updates a certain length value associated data structure has been initialized, which allows local users to obtain sensitive information from k recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2018-18281	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Since Linux kernel version 3.2, the mremap() syscall performs TLB flushes after dropping pagetable locks. If removes entries from the pagetables of a task that is in the middle of mremap(), a stale TLB entry can remai access to a physical page after it has been released back to the page allocator and reused. This is fixed in th 4.9.135, 4.14.78, 4.18.16, 4.19.
CVE-2018-18281	perf-3.10.0-1127.13.1.el7.x86_64	perf	Since Linux kernel version 3.2, the mremap() syscall performs TLB flushes after dropping pagetable locks. If removes entries from the pagetables of a task that is in the middle of mremap(), a stale TLB entry can remai access to a physical page after it has been released back to the page allocator and reused. This is fixed in th 4.9.135, 4.14.78, 4.18.16, 4.19.
CVE-2016-8633	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	drivers/firewire/net.c in the Linux kernel before 4.8.7, in certain unusual hardware configurations, allows remo arbitrary code via crafted fragmented packets.
CVE-2016-8633	perf-3.10.0-1127.13.1.el7.x86_64	perf	drivers/firewire/net.c in the Linux kernel before 4.8.7, in certain unusual hardware configurations, allows remo arbitrary code via crafted fragmented packets.
CVE-2015-8539	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The KEYS subsystem in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of keyctl commands that negatively instantiate a key, related to security/keys/encrypted-keys/encrypted.c, secu security/keys/user_defined.c.
CVE-2015-8539	perf-3.10.0-1127.13.1.el7.x86_64	perf	The KEYS subsystem in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of keyctl commands that negatively instantiate a key, related to security/keys/encrypted-keys/encrypted.c, secu security/keys/user_defined.c.
CVE-2017-10661	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Race condition in fs/timerfd.c in the Linux kernel before 4.10.15 allows local users to gain privileges or cause corruption or use-after-free) via simultaneous file-descriptor operations that leverage improper might_cancel
CVE-2017-10661	perf-3.10.0-1127.13.1.el7.x86_64	perf	Race condition in fs/timerfd.c in the Linux kernel before 4.10.15 allows local users to gain privileges or cause corruption or use-after-free) via simultaneous file-descriptor operations that leverage improper might_cancel
CVE-2019-3882	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the Linux kernel's vfio interface implementation that permits violation of the user's locked bound to a vfio driver, such as vfio-pci, and the local attacker is administratively granted ownership of the de memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.
CVE-2019-3882	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the Linux kernel's vfio interface implementation that permits violation of the user's locked bound to a vfio driver, such as vfio-pci, and the local attacker is administratively granted ownership of the de memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.
CVE-2014-8480	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The instruction decoder in arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel before 3.18-rc2 flags for certain RIP-relative instructions, which allows guest OS users to cause a denial of service (NULL po crash) via a crafted application.
CVE-2014-8480	perf-3.10.0-1127.13.1.el7.x86_64	perf	The instruction decoder in arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel before 3.18-rc2 flags for certain RIP-relative instructions, which allows guest OS users to cause a denial of service (NULL po crash) via a crafted application.
CVE-2018-1094	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.15.15 does not always initialize th which allows attackers to cause a denial of service (ext4_xattr_inode_hash NULL pointer dereference and sy image.
CVE-2018-1094	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.15.15 does not always initialize th which allows attackers to cause a denial of service (ext4_xattr_inode_hash NULL pointer dereference and sy image.
CVE-2017-1000	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	• • This candidate has been reserved by an organization or individual that will use it when announcing a n candidate has been publicized, the details for this candidate will be provided.
CVE-2017-1000	perf-3.10.0-1127.13.1.el7.x86_64	perf	• • This candidate has been reserved by an organization or individual that will use it when announcing a n candidate has been publicized, the details for this candidate will be provided.
CVE-2018-7755	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in the fd_locked_ioctl function in drivers/block/floppy.c in the Linux kernel through 4 copy a kernel pointer to user memory in response to the FDGETPRM ioctl. An attacker can send the FDGET kernel pointer to discover the location of kernel code and data and bypass kernel security protections such a
CVE-2018-7755	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in the fd_locked_ioctl function in drivers/block/floppy.c in the Linux kernel through 4 copy a kernel pointer to user memory in response to the FDGETPRM ioctl. An attacker can send the FDGET kernel pointer to discover the location of kernel code and data and bypass kernel security protections such a

CVE-2015-1421	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Use-after-free vulnerability in the sctp_assoc_update function in net/sctp/associola.c in the Linux kernel befo attackers to cause a denial of service (slab corruption and panic) or possibly have unspecified other impact b that leads to improper handling of shared-key data.
CVE-2015-1421	perf-3.10.0-1127.13.1.el7.x86_64	perf	Use-after-free vulnerability in the sctp_assoc_update function in net/sctp/associola.c in the Linux kernel befo attackers to cause a denial of service (slab corruption and panic) or possibly have unspecified other impact b that leads to improper handling of shared-key data.
CVE-2013-4348	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The skb_flow_dissect function in net/core/flow_dissector.c in the Linux kernel through 3.12 allows remote att service (infinite loop) via a small value in the IHL field of a packet with IPIP encapsulation.
CVE-2013-4348	perf-3.10.0-1127.13.1.el7.x86_64	perf	The skb_flow_dissect function in net/core/flow_dissector.c in the Linux kernel through 3.12 allows remote att service (infinite loop) via a small value in the IHL field of a packet with IPIP encapsulation.
CVE-2018-9363	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the hidp_process_report in bluetooth, there is an integer overflow. This could lead to an out of bounds writ privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel References: Upstream kernel.
CVE-2018-9363	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the hidp_process_report in bluetooth, there is an integer overflow. This could lead to an out of bounds writ privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel References: Upstream kernel.
CVE-2019-11884	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The do_hidp_sock_ioctl function in net/bluetooth/hidp/sock.c in the Linux kernel before 5.0.15 allows a local sensitive information from kernel stack memory via a HIDPCONNADD command, because a name field may
CVE-2019-11884	perf-3.10.0-1127.13.1.el7.x86_64	perf	The do_hidp_sock_ioctl function in net/bluetooth/hidp/sock.c in the Linux kernel before 5.0.15 allows a local sensitive information from kernel stack memory via a HIDPCONNADD command, because a name field may
CVE-2018-9517	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In pppol2tp_connect, there is possible memory corruption due to a use after free. This could lead to local esc execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: And A-38159931.
CVE-2018-9517	perf-3.10.0-1127.13.1.el7.x86_64	perf	In pppol2tp_connect, there is possible memory corruption due to a use after free. This could lead to local esc execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: And A-38159931.
CVE-2018-8897	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB excep SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen config Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpo exceptions until the instruction boundary following the next instruction (SDM Vol. 3A; section 6.8.3). (The inh those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions a enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or PO instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may unexpected behavior when it occurs.
CVE-2018-8897	perf-3.10.0-1127.13.1.el7.x86_64	perf	A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB excep SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen config Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpo exceptions until the instruction boundary following the next instruction (SDM Vol. 3A; section 6.8.3). (The inh those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions a enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or PO instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may unexpected behavior when it occurs.
CVE-2017-2596	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The nested_vmx_check_vmptr function in arch/x86/kvm/vmx.c in the Linux kernel through 4.9.8 improperly e instruction, which allows KVM L1 guest OS users to cause a denial of service (host OS memory consumptio mishandling of page references.
CVE-2017-2596	perf-3.10.0-1127.13.1.el7.x86_64	perf	The nested_vmx_check_vmptr function in arch/x86/kvm/vmx.c in the Linux kernel through 4.9.8 improperly e instruction, which allows KVM L1 guest OS users to cause a denial of service (host OS memory consumptio mishandling of page references.
CVE-2015-0275	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ext4_zero_range function in fs/ext4/extents.c in the Linux kernel before 4.1 allows local users to cause a crafted fallocate zero-range request.
CVE-2015-0275	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ext4_zero_range function in fs/ext4/extents.c in the Linux kernel before 4.1 allows local users to cause a crafted fallocate zero-range request.
CVE-2018-13053	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The alarm_timer_nsleep function in kernel/time/alarmtimer.c in the Linux kernel through 4.17.3 has an intege timeout because ktime_add_safe is not used.
CVE-2018-13053	perf-3.10.0-1127.13.1.el7.x86_64	perf	The alarm_timer_nsleep function in kernel/time/alarmtimer.c in the Linux kernel through 4.17.3 has an intege timeout because ktime_add_safe is not used.
CVE-2014-0100	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Race condition in the inet_frag_intern function in net/ipv4/inet_fragment.c in the Linux kernel through 3.13.6 cause a denial of service (use-after-free error) or possibly have unspecified other impact via a large series of Request packets to a system with a heavy CPU load.
CVE-2014-0100	perf-3.10.0-1127.13.1.el7.x86_64	perf	Race condition in the inet_frag_intern function in net/ipv4/inet_fragment.c in the Linux kernel through 3.13.6 cause a denial of service (use-after-free error) or possibly have unspecified other impact via a large series of Request packets to a system with a heavy CPU load.
CVE-2019-15239	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the Linux kernel, a certain net/ipv4/tcp_output.c change, which was properly incorporated into 4.16.12, wa earlier longterm kernels, introducing a new vulnerability that was potentially more severe than the issue that backporting. Specifically, by adding to a write queue between disconnection and re-connection, a local attack use-after-free conditions. This can result in a kernel crash, or potentially in privilege escalation. NOTE: this a distributions that use 4.9.x longterm kernels before 4.9.190 or 4.14.x longterm kernels before 4.14.139.

CVE-2019-15239	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the Linux kernel, a certain net/ipv4/tcp_output.c change, which was properly incorporated into 4.16.12, wa earlier longterm kernels, introducing a new vulnerability that was potentially more severe than the issue that backporting. Specifically, by adding to a write queue between disconnection and re-connection, a local attack use-after-free conditions. This can result in a kernel crash, or potentially in privilege escalation. NOTE: this a distributions that use 4.9.x longterm kernels before 4.9.190 or 4.14.x longterm kernels before 4.14.139.
CVE-2018-20169	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 4.19.9. The USB subsystem mishandles size checks duri descriptor, related to __usb_get_extra_descriptor in drivers/usb/core/usb.c.
CVE-2018-20169	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 4.19.9. The USB subsystem mishandles size checks duri descriptor, related to __usb_get_extra_descriptor in drivers/usb/core/usb.c.
CVE-2013-6380	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The aac_send_raw_srb function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 3.12.1 does no size value, which allows local users to cause a denial of service (invalid pointer dereference) or possibly have an FSACTL_SEND_RAW_SRB ioctl call that triggers a crafted SRB command.
CVE-2013-6380	perf-3.10.0-1127.13.1.el7.x86_64	perf	The aac_send_raw_srb function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 3.12.1 does no size value, which allows local users to cause a denial of service (invalid pointer dereference) or possibly have an FSACTL_SEND_RAW_SRB ioctl call that triggers a crafted SRB command.
CVE-2017-18232	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Serial Attached SCSI (SAS) implementation in the Linux kernel through 4.15.9 mishandles a mutex withi users to cause a denial of service (deadlock) by triggering certain error-handling code.
CVE-2017-18232	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Serial Attached SCSI (SAS) implementation in the Linux kernel through 4.15.9 mishandles a mutex withi users to cause a denial of service (deadlock) by triggering certain error-handling code.
CVE-2016-10208	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.9.8 does not properly validate me physically proximate attackers to cause a denial of service (out-of-bounds read and system crash) via a craft
CVE-2016-10208	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.9.8 does not properly validate me physically proximate attackers to cause a denial of service (out-of-bounds read and system crash) via a craft
CVE-2018-1118	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Linux kernel vhost since version 4.8 does not properly initialize memory in messages passed between virtual system in the vhost/vhost.c:vhost_new_msg() function. This can allow local privileged users to read some ke reading from the /dev/vhost-net device file.
CVE-2018-1118	perf-3.10.0-1127.13.1.el7.x86_64	perf	Linux kernel vhost since version 4.8 does not properly initialize memory in messages passed between virtual system in the vhost/vhost.c:vhost_new_msg() function. This can allow local privileged users to read some ke reading from the /dev/vhost-net device file.
CVE-2019-14283	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the Linux kernel before 5.2.3, set_geometry in drivers/block/floppy.c does not validate the sect and head fi integer overflow and out-of-bounds read. It can be triggered by an unprivileged local user when a floppy disk QEMU creates the floppy device by default.
CVE-2019-14283	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the Linux kernel before 5.2.3, set_geometry in drivers/block/floppy.c does not validate the sect and head fi integer overflow and out-of-bounds read. It can be triggered by an unprivileged local user when a floppy disk QEMU creates the floppy device by default.
CVE-2013-4563	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The udp6_ufo_fragment function in net/ipv6/udp_offload.c in the Linux kernel through 3.12, when UDP Fragr enabled, does not properly perform a certain size comparison before inserting a fragment header, which allow denial of service (panic) via a large IPv6 UDP packet, as demonstrated by use of the Token Bucket Filter (TE
CVE-2013-4563	perf-3.10.0-1127.13.1.el7.x86_64	perf	The udp6_ufo_fragment function in net/ipv6/udp_offload.c in the Linux kernel through 3.12, when UDP Fragr enabled, does not properly perform a certain size comparison before inserting a fragment header, which allow denial of service (panic) via a large IPv6 UDP packet, as demonstrated by use of the Token Bucket Filter (TE
CVE-2014-1438	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The restore_fpu_checking function in arch/x86/include/asm/fpu-internal.h in the Linux kernel before 3.12.8 or does not clear pending exceptions before proceeding to an EMMS instruction, which allows local users to ca kill) or possibly gain privileges via a crafted application.
CVE-2014-1438	perf-3.10.0-1127.13.1.el7.x86_64	perf	The restore_fpu_checking function in arch/x86/include/asm/fpu-internal.h in the Linux kernel before 3.12.8 or does not clear pending exceptions before proceeding to an EMMS instruction, which allows local users to ca kill) or possibly gain privileges via a crafted application.
CVE-2018-14633	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A security flaw was found in the chap_server_compute_md5() function in the ISCSI target code in the Linux k authentication request from an ISCSI initiator is processed. An unauthenticated remote attacker can cause a smash up to 17 bytes of the stack. The attack requires the iSCSI target to be enabled on the victim host. Dep code was built (i.e. depending on a compiler, compile flags and hardware architecture) an attack may lead to denial-of-service or possibly to a non-authorized access to data exported by an iSCSI target. Due to the natu escalation cannot be fully ruled out, although we believe it is highly unlikely. Kernel versions 4.18.x, 4.14.x ar vulnerable.
CVE-2018-14633	perf-3.10.0-1127.13.1.el7.x86_64	perf	A security flaw was found in the chap_server_compute_md5() function in the ISCSI target code in the Linux k authentication request from an ISCSI initiator is processed. An unauthenticated remote attacker can cause a smash up to 17 bytes of the stack. The attack requires the iSCSI target to be enabled on the victim host. Dep code was built (i.e. depending on a compiler, compile flags and hardware architecture) an attack may lead to denial-of-service or possibly to a non-authorized access to data exported by an iSCSI target. Due to the natu escalation cannot be fully ruled out, although we believe it is highly unlikely. Kernel versions 4.18.x, 4.14.x ar vulnerable.
CVE-2014-0102	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The keyring_detect_cycle_iterator function in security/keys/keyring.c in the Linux kernel through 3.13.6 does keyrings are identical, which allows local users to cause a denial of service (OOPS) via crafted keyctl comma
CVE-2014-0102	perf-3.10.0-1127.13.1.el7.x86_64	perf	The keyring_detect_cycle_iterator function in security/keys/keyring.c in the Linux kernel through 3.13.6 does keyrings are identical, which allows local users to cause a denial of service (OOPS) via crafted keyctl comma

CVE-2019-10639	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel addr KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the IP ID values th connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP address collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key co address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is carried out remotely, by the attacker forcing the target device to send UDP or ICMP (or certain other) traffic t addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can b attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because IP ID gen dependency on an address associated with a network namespace.
CVE-2019-10639	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel addr KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the IP ID values th connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP address collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key co address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is carried out remotely, by the attacker forcing the target device to send UDP or ICMP (or certain other) traffic t addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can b attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because IP ID gen dependency on an address associated with a network namespace.
CVE-2013-7421	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bin socket with a module name in the salg_name field, a different vulnerability than CVE-2014-9644.
CVE-2013-7421	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bin socket with a module name in the salg_name field, a different vulnerability than CVE-2014-9644.
CVE-2018-16658	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 4.18.6. An information leak in cdrom_ioctl_drive_status ir be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bo to CVE-2018-10940.
CVE-2018-16658	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 4.18.6. An information leak in cdrom_ioctl_drive_status ir be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bo to CVE-2018-10940.
CVE-2017-7477	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Heap-based buffer overflow in drivers/net/macsec.c in the MACsec module in the Linux kernel through 4.10.1 denial of service or possibly have unspecified other impact by leveraging the use of a MAX_SKB_FRAGS+1 NETIF_F_FRAGLIST feature, leading to an error in the skb_to_sgvec function.
CVE-2017-7477	perf-3.10.0-1127.13.1.el7.x86_64	perf	Heap-based buffer overflow in drivers/net/macsec.c in the MACsec module in the Linux kernel through 4.10.1 denial of service or possibly have unspecified other impact by leveraging the use of a MAX_SKB_FRAGS+1 NETIF_F_FRAGLIST feature, leading to an error in the skb_to_sgvec function.
CVE-2019-15916	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 5.0.1. There is a memory leak in register_queue_kobject which will cause denial of service.
CVE-2019-15916	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 5.0.1. There is a memory leak in register_queue_kobject which will cause denial of service.
CVE-2018-5344	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the Linux kernel through 4.14.13, drivers/block/loop.c mishandles lo_release serialization, which allows att service (__lock_acquire use-after-free) or possibly have unspecified other impact.
CVE-2018-5344	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the Linux kernel through 4.14.13, drivers/block/loop.c mishandles lo_release serialization, which allows att service (__lock_acquire use-after-free) or possibly have unspecified other impact.
CVE-2019-19768	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the Linux kernel 5.4.0-rc2, there is a use-after-free (read) in the __blk_add_trace function in kernel/trace/b out a blk_io_trace structure and place it in a per-cpu sub-buffer).
CVE-2019-19768	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the Linux kernel 5.4.0-rc2, there is a use-after-free (read) in the __blk_add_trace function in kernel/trace/b out a blk_io_trace structure and place it in a per-cpu sub-buffer).
CVE-2014-8086	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Race condition in the ext4_file_write_iter function in fs/ext4/file.c in the Linux kernel through 3.17 allows loca service (file unavailability) via a combination of a write action and an F_SETFL fcntl operation for the O_DIRE
CVE-2014-8086	perf-3.10.0-1127.13.1.el7.x86_64	perf	Race condition in the ext4_file_write_iter function in fs/ext4/file.c in the Linux kernel through 3.17 allows loca service (file unavailability) via a combination of a write action and an F_SETFL fcntl operation for the O_DIRE
CVE-2017-13215	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A elevation of privilege vulnerability in the Upstream kernel skcipher. Product: Android. Versions: Android ke References: Upstream kernel.
CVE-2017-13215	perf-3.10.0-1127.13.1.el7.x86_64	perf	A elevation of privilege vulnerability in the Upstream kernel skcipher. Product: Android. Versions: Android ke References: Upstream kernel.
CVE-2013-7026	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Multiple race conditions in ipc/shm.c in the Linux kernel before 3.12.2 allow local users to cause a denial of s system crash) or possibly have unspecified other impact via a crafted application that uses shmctl IPC_RMID other shm system calls.
CVE-2013-7026	perf-3.10.0-1127.13.1.el7.x86_64	perf	Multiple race conditions in ipc/shm.c in the Linux kernel before 3.12.2 allow local users to cause a denial of s system crash) or possibly have unspecified other impact via a crafted application that uses shmctl IPC_RMID other shm system calls.
CVE-2016-4913	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka containing \0 characters, which allows local users to obtain sensitive information from kernel memory or poss impact via a crafted isofs filesystem.
CVE-2016-4913	perf-3.10.0-1127.13.1.el7.x86_64	perf	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka containing \0 characters, which allows local users to obtain sensitive information from kernel memory or poss impact via a crafted isofs filesystem.

CVE-2016-9806	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg operation associated with a new dump that started earlier than anticipated.
CVE-2016-9806	perf-3.10.0-1127.13.1.el7.x86_64	perf	Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg operation associated with a new dump that started earlier than anticipated.
CVE-2020-10711	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_ attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to cras in a denial of service.
CVE-2020-10711	perf-3.10.0-1127.13.1.el7.x86_64	perf	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_ attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to cras in a denial of service.
CVE-2018-1120	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found affecting the Linux kernel before version 4.17. By mmap()ing a FUSE-backed file onto a pr command line arguments (or environment strings), an attacker can cause utilities from psutils or procps (suc program which makes a read() call to the /proc/<pid>/cmdline (or /proc/<pid>/environ) files to block indefinite some controlled time (as a synchronization primitive for other attacks).
CVE-2018-1120	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found affecting the Linux kernel before version 4.17. By mmap()ing a FUSE-backed file onto a pr command line arguments (or environment strings), an attacker can cause utilities from psutils or procps (suc program which makes a read() call to the /proc/<pid>/cmdline (or /proc/<pid>/environ) files to block indefinite some controlled time (as a synchronization primitive for other attacks).
CVE-2018-18559	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the Linux kernel through 4.19, a use-after-free can occur due to a race condition between fanout_add from AF_PACKET socket. This issue exists because of the 15fe076edea787807a7cdc168df832544b58eba6 inco The code mishandles a certain multithreaded case involving a packet_do_bind unregister action followed by action. Later, packet_release operates on only one of the two applicable linked lists. The attacker can achiev
CVE-2018-18559	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the Linux kernel through 4.19, a use-after-free can occur due to a race condition between fanout_add from AF_PACKET socket. This issue exists because of the 15fe076edea787807a7cdc168df832544b58eba6 inco The code mishandles a certain multithreaded case involving a packet_do_bind unregister action followed by action. Later, packet_release operates on only one of the two applicable linked lists. The attacker can achiev
CVE-2014-3534	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	arch/s390/kernel/ptrace.c in the Linux kernel before 3.15.8 on the s390 platform does not properly restrict ad in PTRACE_POKEUSR_AREA requests, which allows local users to obtain read and write access to kernel consequently gain privileges, via a crafted application that makes a ptrace system call.
CVE-2014-3534	perf-3.10.0-1127.13.1.el7.x86_64	perf	arch/s390/kernel/ptrace.c in the Linux kernel before 3.15.8 on the s390 platform does not properly restrict ad in PTRACE_POKEUSR_AREA requests, which allows local users to obtain read and write access to kernel consequently gain privileges, via a crafted application that makes a ptrace system call.
CVE-2020-0543	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an enable information disclosure via local access.
CVE-2020-0543	perf-3.10.0-1127.13.1.el7.x86_64	perf	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an enable information disclosure via local access.
CVE-2013-4127	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Use-after-free vulnerability in the vhost_net_set_backend function in drivers/vhost/net.c in the Linux kernel th to cause a denial of service (OOPS and system crash) via vectors involving powering on a virtual machine.
CVE-2013-4127	perf-3.10.0-1127.13.1.el7.x86_64	perf	Use-after-free vulnerability in the vhost_net_set_backend function in drivers/vhost/net.c in the Linux kernel th to cause a denial of service (OOPS and system crash) via vectors involving powering on a virtual machine.
CVE-2019-11091	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some micropro execution may allow an authenticated user to potentially enable information disclosure via a side channel wit impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-
CVE-2019-11091	perf-3.10.0-1127.13.1.el7.x86_64	perf	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some micropro execution may allow an authenticated user to potentially enable information disclosure via a side channel wit impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-
CVE-2018-10940	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows l incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory.
CVE-2018-10940	perf-3.10.0-1127.13.1.el7.x86_64	perf	The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows l incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory.
CVE-2017-5970	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attacker (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP
CVE-2017-5970	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attacker (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP
CVE-2016-10147	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	crypto/mcryptd.c in the Linux kernel before 4.8.15 allows local users to cause a denial of service (NULL poin crash) by using an AF_ALG socket with an incompatible algorithm, as demonstrated by mcryptd(md5).
CVE-2016-10147	perf-3.10.0-1127.13.1.el7.x86_64	perf	crypto/mcryptd.c in the Linux kernel before 4.8.15 allows local users to cause a denial of service (NULL poin crash) by using an AF_ALG socket with an incompatible algorithm, as demonstrated by mcryptd(md5).

CVE-2013-4163	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ip6_append_data_mtu function in net/ipv6/ip6_output.c in the IPv6 implementation in the Linux kernel th maintain information about whether the IPV6_MTU setsockopt option had been specified, which allows local service (BUG and system crash) via a crafted application that uses the UDP_CORK option in a setsockopt s
CVE-2013-4163	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ip6_append_data_mtu function in net/ipv6/ip6_output.c in the IPv6 implementation in the Linux kernel th maintain information about whether the IPV6_MTU setsockopt option had been specified, which allows local service (BUG and system crash) via a crafted application that uses the UDP_CORK option in a setsockopt s
CVE-2017-1000380	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	sound/core/timer.c in the Linux kernel before 4.11.5 is vulnerable to a data race in the ALSA /dev/snd/timer c being able to read information belonging to other users, i.e., uninitialized memory contents may be disclosed happen at the same time.
CVE-2017-1000380	perf-3.10.0-1127.13.1.el7.x86_64	perf	sound/core/timer.c in the Linux kernel before 4.11.5 is vulnerable to a data race in the ALSA /dev/snd/timer c being able to read information belonging to other users, i.e., uninitialized memory contents may be disclosed happen at the same time.
CVE-2014-9644	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bin socket with a parenthesized module template expression in the salg_name field, as demonstrated by the vfa vulnerability than CVE-2013-7421.
CVE-2014-9644	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Crypto API in the Linux kernel before 3.18.5 allows local users to load arbitrary kernel modules via a bin socket with a parenthesized module template expression in the salg_name field, as demonstrated by the vfa vulnerability than CVE-2013-7421.
CVE-2014-3181	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Multiple stack-based buffer overflows in the magicmouse_raw_event function in drivers/hid/hid-magicmouse. driver in the Linux kernel through 3.16.3 allow physically proximate attackers to cause a denial of service (sy arbitrary code via a crafted device that provides a large amount of (1) EHCI or (2) XHCI data associated with
CVE-2014-3181	perf-3.10.0-1127.13.1.el7.x86_64	perf	Multiple stack-based buffer overflows in the magicmouse_raw_event function in drivers/hid/hid-magicmouse. driver in the Linux kernel through 3.16.3 allow physically proximate attackers to cause a denial of service (sy arbitrary code via a crafted device that provides a large amount of (1) EHCI or (2) XHCI data associated with
CVE-2014-7145	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The SMB2_tcon function in fs/cifs/smb2pdu.c in the Linux kernel before 3.16.3 allows remote CIFS servers t (NULL pointer dereference and client system crash) or possibly have unspecified other impact by deleting th of DFS referrals.
CVE-2014-7145	perf-3.10.0-1127.13.1.el7.x86_64	perf	The SMB2_tcon function in fs/cifs/smb2pdu.c in the Linux kernel before 3.16.3 allows remote CIFS servers t (NULL pointer dereference and client system crash) or possibly have unspecified other impact by deleting th of DFS referrals.
CVE-2018-5848	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the function wmi_set_ie(), the length validation code does not handle unsigned integer overflow properly. A 'ie_len' argument can cause a buffer overflow in all Android releases from CAF (Android for MSM, Firefox OS the Linux Kernel.
CVE-2018-5848	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the function wmi_set_ie(), the length validation code does not handle unsigned integer overflow properly. A 'ie_len' argument can cause a buffer overflow in all Android releases from CAF (Android for MSM, Firefox OS the Linux Kernel.
CVE-2018-13095	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.17.3. A denial of servic BUG) can occur for a corrupted xfs image upon encountering an inode that is in extent format, but has more fork.
CVE-2018-13095	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.17.3. A denial of servic BUG) can occur for a corrupted xfs image upon encountering an inode that is in extent format, but has more fork.
CVE-2017-17805	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inp able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequen blkcipher_walk API. Both the generic implementation (crypto/salsa20_generic.c) and x86 implementation (ar of Salsa20 were vulnerable.
CVE-2017-17805	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inp able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequen blkcipher_walk API. Both the generic implementation (crypto/salsa20_generic.c) and x86 implementation (ar of Salsa20 were vulnerable.
CVE-2013-7267	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The atalk_recvmsg function in net/appletalk/ddp.c in the Linux kernel before 3.12.4 updates a certain length associated data structure has been initialized, which allows local users to obtain sensitive information from k recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2013-7267	perf-3.10.0-1127.13.1.el7.x86_64	perf	The atalk_recvmsg function in net/appletalk/ddp.c in the Linux kernel before 3.12.4 updates a certain length associated data structure has been initialized, which allows local users to obtain sensitive information from k recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2019-11811	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 5.0.4. There is a use-after-free upon attempted read acce ipmi_si module is removed, related to drivers/char/ipmi/ipmi_si_intf.c, drivers/char/ipmi/ipmi_si_mem_io.c, ar drivers/char/ipmi/ipmi_si_port_io.c.
CVE-2019-11811	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 5.0.4. There is a use-after-free upon attempted read acce ipmi_si module is removed, related to drivers/char/ipmi/ipmi_si_intf.c, drivers/char/ipmi/ipmi_si_mem_io.c, ar drivers/char/ipmi/ipmi_si_port_io.c.
CVE-2019-3901	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A race condition in perf_event_open() allows local attackers to leak sensitive data from setuid programs. As the cred_guard_mutex) are held during the ptrace_may_access() call, it is possible for the specified target ta syscall with setuid execution before perf_event_alloc() actually attaches to it, allowing an attacker to bypass and the perf_event_exit_task(current) call that is performed in install_exec_creds() during privileged execve(versions before 4.8.

CVE-2019-3901	perf-3.10.0-1127.13.1.el7.x86_64	perf	A race condition in perf_event_open() allows local attackers to leak sensitive data from setuid programs. As the cred_guard_mutex) are held during the ptrace_may_access() call, it is possible for the specified target ta syscall with setuid execution before perf_event_alloc() actually attaches to it, allowing an attacker to bypass and the perf_event_exit_task(current) call that is performed in install_exec_creds() during privileged execve(versions before 4.8.
CVE-2017-7472	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (mem of KEY_REQKEY_DEFL_THREAD_KEYRING keyctl_set_reqkey_keyring calls.
CVE-2017-7472	perf-3.10.0-1127.13.1.el7.x86_64	perf	The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (mem of KEY_REQKEY_DEFL_THREAD_KEYRING keyctl_set_reqkey_keyring calls.
CVE-2015-8970	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	crypto/algif_skcipher.c in the Linux kernel before 4.4.2 does not verify that a setkey operation has been perfo before an accept system call is processed, which allows local users to cause a denial of service (NULL point crash) via a crafted application that does not supply a key, related to the lrw_crypt function in crypto/lrw.c.
CVE-2015-8970	perf-3.10.0-1127.13.1.el7.x86_64	perf	crypto/algif_skcipher.c in the Linux kernel before 4.4.2 does not verify that a setkey operation has been perfo before an accept system call is processed, which allows local users to cause a denial of service (NULL point crash) via a crafted application that does not supply a key, related to the lrw_crypt function in crypto/lrw.c.
CVE-2018-1000199	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Linux Kernel version 3.18 contains a dangerous feature vulnerability in modify_user_hw_breakpoint() tha possibly memory corruption. This attack appear to be exploitable via local code execution and the ability to u appears to have been fixed in git commit f67b15037a7a50c57f72e69a6d59941ad90a0f0f.
CVE-2018-1000199	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Linux Kernel version 3.18 contains a dangerous feature vulnerability in modify_user_hw_breakpoint() tha possibly memory corruption. This attack appear to be exploitable via local code execution and the ability to u appears to have been fixed in git commit f67b15037a7a50c57f72e69a6d59941ad90a0f0f.
CVE-2014-3647	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel through 3.17.2 does not properly perform guest OS users to cause a denial of service (guest OS crash) via a crafted application.
CVE-2014-3647	perf-3.10.0-1127.13.1.el7.x86_64	perf	arch/x86/kvm/emulate.c in the KVM subsystem in the Linux kernel through 3.17.2 does not properly perform guest OS users to cause a denial of service (guest OS crash) via a crafted application.
CVE-2014-4171	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	mm/shmem.c in the Linux kernel through 3.15.1 does not properly implement the interaction between range which allows local users to cause a denial of service (i_mutex hold) by using the mmap system call to access interfering with intended shmem activity by blocking completion of (1) an MADV_REMOVE madvise call or (2 FALLOC_FL_PUNCH_HOLE fallocate call.
CVE-2014-4171	perf-3.10.0-1127.13.1.el7.x86_64	perf	mm/shmem.c in the Linux kernel through 3.15.1 does not properly implement the interaction between range which allows local users to cause a denial of service (i_mutex hold) by using the mmap system call to access interfering with intended shmem activity by blocking completion of (1) an MADV_REMOVE madvise call or (2 FALLOC_FL_PUNCH_HOLE fallocate call.
CVE-2015-1333	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Memory leak in the __key_link_end function in security/keys/keyring.c in the Linux kernel before 4.1.4 allows service (memory consumption) via many add_key system calls that refer to existing keys.
CVE-2015-1333	perf-3.10.0-1127.13.1.el7.x86_64	perf	Memory leak in the __key_link_end function in security/keys/keyring.c in the Linux kernel before 4.1.4 allows service (memory consumption) via many add_key system calls that refer to existing keys.
CVE-2015-5283	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The sctp_init function in net/sctp/protocol.c in the Linux kernel before 4.2.3 has an incorrect sequence of prot allows local users to cause a denial of service (panic or memory corruption) by creating SCTP sockets before
CVE-2015-5283	perf-3.10.0-1127.13.1.el7.x86_64	perf	The sctp_init function in net/sctp/protocol.c in the Linux kernel before 4.2.3 has an incorrect sequence of prot allows local users to cause a denial of service (panic or memory corruption) by creating SCTP sockets before
CVE-2016-7913	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The xc2028_set_config function in drivers/media/tuners/tuner-xc2028.c in the Linux kernel before 4.6 allows cause a denial of service (use-after-free) via vectors involving omission of the firmware name from a certain
CVE-2016-7913	perf-3.10.0-1127.13.1.el7.x86_64	perf	The xc2028_set_config function in drivers/media/tuners/tuner-xc2028.c in the Linux kernel before 4.6 allows cause a denial of service (use-after-free) via vectors involving omission of the firmware name from a certain
CVE-2017-5986	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allo denial of service (assertion failure and panic) via a multithreaded application that peels off an association in a
CVE-2017-5986	perf-3.10.0-1127.13.1.el7.x86_64	perf	Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allo denial of service (assertion failure and panic) via a multithreaded application that peels off an association in a
CVE-2018-9516	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In hid_debug_events_read of drivers/hid/hid-debug.c, there is a possible out of bounds write due to a missing lead to local escalation of privilege with System execution privileges needed. User interaction is not needed f Android Versions: Android kernel Android ID: A-71361580.
CVE-2018-9516	perf-3.10.0-1127.13.1.el7.x86_64	perf	In hid_debug_events_read of drivers/hid/hid-debug.c, there is a possible out of bounds write due to a missing lead to local escalation of privilege with System execution privileges needed. User interaction is not needed f Android Versions: Android kernel Android ID: A-71361580.
CVE-2019-10638	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the IP ID values the kernel pro protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conduc page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.
CVE-2019-10638	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the IP ID values the kernel pro protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conduc page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.
CVE-2013-4343	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Use-after-free vulnerability in drivers/net/tun.c in the Linux kernel through 3.11.1 allows local users to gain pr CAP_NET_ADMIN capability and providing an invalid tuntap interface name in a TUNSETIFF ioctl call.

CVE-2013-4343	perf-3.10.0-1127.13.1.el7.x86_64	perf	Use-after-free vulnerability in drivers/net/tun.c in the Linux kernel through 3.11.1 allows local users to gain pr CAP_NET_ADMIN capability and providing an invalid tuntap interface name in a TUNSETIFF ioctl call.
CVE-2019-9500	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Broadcom brcmfmac WiFi driver prior to commit 1b5e2423164b3670e8bc9174e4762d297990deff is vuln overflow. If the Wake-up on Wireless LAN functionality is configured, a malicious event frame can be constru overflow in the brcmf_wowl_nd_results function. This vulnerability can be exploited with compromised chipse when used in combination with CVE-2019-9503, can be used remotely. In the worst case scenario, by sendi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. M will result in denial-of-service conditions.
CVE-2019-9500	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Broadcom brcmfmac WiFi driver prior to commit 1b5e2423164b3670e8bc9174e4762d297990deff is vuln overflow. If the Wake-up on Wireless LAN functionality is configured, a malicious event frame can be constru overflow in the brcmf_wowl_nd_results function. This vulnerability can be exploited with compromised chipse when used in combination with CVE-2019-9503, can be used remotely. In the worst case scenario, by sendi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. M will result in denial-of-service conditions.
CVE-2014-4014	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The capabilities implementation in the Linux kernel before 3.14.8 does not properly consider that namespace which allows local users to bypass intended chmod restrictions by first creating a user namespace, as demon on a file with group ownership of root.
CVE-2014-4014	perf-3.10.0-1127.13.1.el7.x86_64	perf	The capabilities implementation in the Linux kernel before 3.14.8 does not properly consider that namespace which allows local users to bypass intended chmod restrictions by first creating a user namespace, as demon on a file with group ownership of root.
CVE-2018-1091	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the flush_tmregs_to_thread function in arch/powerpc/kernel/ptrace.c in the Linux kernel before 4.13.5, a gu triggered from unprivileged userspace during a core dump on a POWER host due to a missing processor fea use of transactional memory (TM) instructions in the core dump path, leading to a denial of service.
CVE-2018-1091	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the flush_tmregs_to_thread function in arch/powerpc/kernel/ptrace.c in the Linux kernel before 4.13.5, a gu triggered from unprivileged userspace during a core dump on a POWER host due to a missing processor fea use of transactional memory (TM) instructions in the core dump path, leading to a denial of service.
CVE-2018-7191	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the tun subsystem in the Linux kernel before 4.13.14, dev_get_valid_name is not called before register_ne to cause a denial of service (NULL pointer dereference and panic) via an ioctl(TUNSETIFF) call with a dev na This is similar to CVE-2013-4343.
CVE-2018-7191	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the tun subsystem in the Linux kernel before 4.13.14, dev_get_valid_name is not called before register_ne to cause a denial of service (NULL pointer dereference and panic) via an ioctl(TUNSETIFF) call with a dev na This is similar to CVE-2013-4343.
CVE-2014-3186	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Buffer overflow in the picolcd_raw_event function in devices/hid/hid-picolcd_core.c in the PicoLCD HID devic through 3.16.3, as used in Android on Nexus 7 devices, allows physically proximate attackers to cause a den possibly execute arbitrary code via a crafted device that sends a large report.
CVE-2014-3186	perf-3.10.0-1127.13.1.el7.x86_64	perf	Buffer overflow in the picolcd_raw_event function in devices/hid/hid-picolcd_core.c in the PicoLCD HID devic through 3.16.3, as used in Android on Nexus 7 devices, allows physically proximate attackers to cause a den possibly execute arbitrary code via a crafted device that sends a large report.
CVE-2016-9793	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative value which allows local users to cause a denial of service (memory corruption and system crash) or possibly have leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFF(SO_RCVBUFFORCE option.
CVE-2016-9793	perf-3.10.0-1127.13.1.el7.x86_64	perf	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative value which allows local users to cause a denial of service (memory corruption and system crash) or possibly have leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFF(SO_RCVBUFFORCE option.
CVE-2014-2309	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ip6_route_add function in net/ipv6/route.c in the Linux kernel through 3.13.6 does not properly count the allows remote attackers to cause a denial of service (memory consumption) via a flood of ICMPv6 Router Ad
CVE-2014-2309	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ip6_route_add function in net/ipv6/route.c in the Linux kernel through 3.13.6 does not properly count the allows remote attackers to cause a denial of service (memory consumption) via a flood of ICMPv6 Router Ad
CVE-2018-16884	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the Linux kernel's NFS41+ subsystem. NFS41+ shares mounted in different network nam make bc_svc_process() use wrong back-channel IDs and cause a use-after-free vulnerability. Thus a malicio host kernel memory corruption and a system panic. Due to the nature of the flaw, privilege escalation cannot
CVE-2018-16884	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the Linux kernel's NFS41+ subsystem. NFS41+ shares mounted in different network nam make bc_svc_process() use wrong back-channel IDs and cause a use-after-free vulnerability. Thus a malicio host kernel memory corruption and a system panic. Due to the nature of the flaw, privilege escalation cannot
CVE-2018-19985	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The function hso_get_config_data in drivers/net/usb/hso.c in the Linux kernel through 4.19.8 reads if_num fr and uses it to index a small array, resulting in an object out-of-bounds (OOB) read that potentially allows arbi space.
CVE-2018-19985	perf-3.10.0-1127.13.1.el7.x86_64	perf	The function hso_get_config_data in drivers/net/usb/hso.c in the Linux kernel through 4.19.8 reads if_num fr and uses it to index a small array, resulting in an object out-of-bounds (OOB) read that potentially allows arbi space.
CVE-2016-9084	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows l service (integer overflow) or have unspecified other impact by leveraging access to a vfio PCI device file.
CVE-2016-9084	perf-3.10.0-1127.13.1.el7.x86_64	perf	drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows l service (integer overflow) or have unspecified other impact by leveraging access to a vfio PCI device file.
CVE-2018-1092	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ext4_iget function in fs/ext4/inode.c in the Linux kernel through 4.15.15 mishandles the case of a root di i_links_count, which allows attackers to cause a denial of service (ext4_process_freed_data NULL pointer de crafted ext4 image.

CVE-2018-1092	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ext4_iget function in fs/ext4/inode.c in the Linux kernel through 4.15.15 mishandles the case of a root di i_links_count, which allows attackers to cause a denial of service (ext4_process_freed_data NULL pointer de crafted ext4 image.
CVE-2018-1000026	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation card driver that can result in DoS: Network card firmware assertion takes card off-line. This attack appear to on a must pass a very large, specially crafted packet to the bnx2x card. This can be done from an untrusted
CVE-2018-1000026	perf-3.10.0-1127.13.1.el7.x86_64	perf	Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation card driver that can result in DoS: Network card firmware assertion takes card off-line. This attack appear to on a must pass a very large, specially crafted packet to the bnx2x card. This can be done from an untrusted
CVE-2017-1219	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	IBM Tivoli Endpoint Manager is vulnerable to a XML External Entity Injection (XXE) attack when processing could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force I
CVE-2017-1219	perf-3.10.0-1127.13.1.el7.x86_64	perf	IBM Tivoli Endpoint Manager is vulnerable to a XML External Entity Injection (XXE) attack when processing could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force I
CVE-2018-15594	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it e Spectre-v2 attacks against paravirtual guests.
CVE-2018-15594	perf-3.10.0-1127.13.1.el7.x86_64	perf	arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it e Spectre-v2 attacks against paravirtual guests.
CVE-2016-4581	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	fs/pnode.c in the Linux kernel before 4.5.4 does not properly traverse a mount propagation tree in a certain c which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted se
CVE-2016-4581	perf-3.10.0-1127.13.1.el7.x86_64	perf	fs/pnode.c in the Linux kernel before 4.5.4 does not properly traverse a mount propagation tree in a certain c which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted se
CVE-2016-7039	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack cor possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demo only VLAN headers, a related issue to CVE-2016-8666.
CVE-2016-7039	perf-3.10.0-1127.13.1.el7.x86_64	perf	The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack cor possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demo only VLAN headers, a related issue to CVE-2016-8666.
CVE-2016-9083	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	drivers/vfio/pci/vfio_pci.c in the Linux kernel through 4.8.11 allows local users to bypass integer overflow che service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file VFIO_DEVICE_SET_IRQS ioctl call, aka a "state machine confusion bug."
CVE-2016-9083	perf-3.10.0-1127.13.1.el7.x86_64	perf	drivers/vfio/pci/vfio_pci.c in the Linux kernel through 4.8.11 allows local users to bypass integer overflow che service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file VFIO_DEVICE_SET_IRQS ioctl call, aka a "state machine confusion bug."
CVE-2013-4350	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The IPv6 SCTP implementation in net/sctp/ipv6.c in the Linux kernel through 3.11.1 uses data structures and trigger an intended configuration of IPsec encryption, which allows remote attackers to obtain sensitive inforr
CVE-2013-4350	perf-3.10.0-1127.13.1.el7.x86_64	perf	The IPv6 SCTP implementation in net/sctp/ipv6.c in the Linux kernel through 3.11.1 uses data structures and trigger an intended configuration of IPsec encryption, which allows remote attackers to obtain sensitive inforr
CVE-2015-1573	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The nft_flush_table function in net/netfilter/nf_tables_api.c in the Linux kernel before 3.18.5 mishandles the ir jumps and ruleset flushes, which allows local users to cause a denial of service (panic) by leveraging the CA
CVE-2015-1573	perf-3.10.0-1127.13.1.el7.x86_64	perf	The nft_flush_table function in net/netfilter/nf_tables_api.c in the Linux kernel before 3.18.5 mishandles the ir jumps and ruleset flushes, which allows local users to cause a denial of service (panic) by leveraging the CA
CVE-2019-7222	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak.
CVE-2019-7222	perf-3.10.0-1127.13.1.el7.x86_64	perf	The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak.
CVE-2016-9604	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	It was discovered in the Linux kernel before 4.11-rc8 that root can gain direct access to an internal keyring, s RHEL-7 or '.builtin_trusted_keys' upstream, by joining it as its session keyring. This allows root to bypass mo adding a new public key of its own devising to the keyring.
CVE-2016-9604	perf-3.10.0-1127.13.1.el7.x86_64	perf	It was discovered in the Linux kernel before 4.11-rc8 that root can gain direct access to an internal keyring, s RHEL-7 or '.builtin_trusted_keys' upstream, by joining it as its session keyring. This allows root to bypass mo adding a new public key of its own devising to the keyring.
CVE-2019-11190	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Linux kernel before 4.8 allows local users to bypass ASLR on setuid programs (such as /bin/su) becaus too late in load_elf_binary() in fs/binfmt_elf.c, and thus the ptrace_may_access() check has a race condition
CVE-2019-11190	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Linux kernel before 4.8 allows local users to bypass ASLR on setuid programs (such as /bin/su) becaus too late in load_elf_binary() in fs/binfmt_elf.c, and thus the ptrace_may_access() check has a race condition
CVE-2015-9289	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	In the Linux kernel before 4.1.4, a buffer overflow occurs when checking userspace params in drivers/media/ maximum size for a DiSEqC command is 6, according to the userspace API. However, the code allows large
CVE-2015-9289	perf-3.10.0-1127.13.1.el7.x86_64	perf	In the Linux kernel before 4.1.4, a buffer overflow occurs when checking userspace params in drivers/media/ maximum size for a DiSEqC command is 6, according to the userspace API. However, the code allows large
CVE-2017-7187	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a deni buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_ out-of-bounds write access in the sg_write function.

CVE-2017-7187	perf-3.10.0-1127.13.1.el7.x86_64	perf	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a deni buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_ out-of-bounds write access in the sg_write function.
CVE-2014-2568	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Use-after-free vulnerability in the nfqnl_zcopy function in net/netfilter/nfnetlink_queue_core.c in the Linux ker attackers to obtain sensitive information from kernel memory by leveraging the absence of a certain orphanir affected code was moved to the skb_zerocopy function in net/core/skbuff.c before the vulnerability was anno
CVE-2014-2568	perf-3.10.0-1127.13.1.el7.x86_64	perf	Use-after-free vulnerability in the nfqnl_zcopy function in net/netfilter/nfnetlink_queue_core.c in the Linux ker attackers to obtain sensitive information from kernel memory by leveraging the absence of a certain orphanir affected code was moved to the skb_zerocopy function in net/core/skbuff.c before the vulnerability was anno
CVE-2018-5750	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The acpi_smbus_hc_add function in drivers/acpi/sbshc.c in the Linux kernel through 4.14.15 allows local use information by reading dmesg data from an SBS HC printk call.
CVE-2018-5750	perf-3.10.0-1127.13.1.el7.x86_64	perf	The acpi_smbus_hc_add function in drivers/acpi/sbshc.c in the Linux kernel through 4.14.15 allows local use information by reading dmesg data from an SBS HC printk call.
CVE-2017-18595	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 4.14.11. A double free may be caused by the function all kernel/trace/trace.c.
CVE-2017-18595	perf-3.10.0-1127.13.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 4.14.11. A double free may be caused by the function all kernel/trace/trace.c.
CVE-2019-9506	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Bluetooth BR/EDR specification up to and including version 5.1 permits sufficiently low encryption key le attacker from influencing the key length negotiation. This allows practical brute-force attacks (aka "KNOB") th arbitrary ciphertext without the victim noticing.
CVE-2019-9506	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Bluetooth BR/EDR specification up to and including version 5.1 permits sufficiently low encryption key le attacker from influencing the key length negotiation. This allows practical brute-force attacks (aka "KNOB") th arbitrary ciphertext without the victim noticing.
CVE-2015-3212	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Race condition in net/sctp/socket.c in the Linux kernel before 4.1.2 allows local users to cause a denial of se via a rapid series of system calls related to sockets, as demonstrated by setsockopt calls.
CVE-2015-3212	perf-3.10.0-1127.13.1.el7.x86_64	perf	Race condition in net/sctp/socket.c in the Linux kernel before 4.1.2 allows local users to cause a denial of se via a rapid series of system calls related to sockets, as demonstrated by setsockopt calls.
CVE-2019-3892	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	• • DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-11599. Reason: This candidate is CVE-2019-11599. Notes: All CVE users should reference CVE-2019-11599 instead of this candidate. A in this candidate have been removed to prevent accidental usage.
CVE-2019-3892	perf-3.10.0-1127.13.1.el7.x86_64	perf	• • DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-11599. Reason: This candidate is CVE-2019-11599. Notes: All CVE users should reference CVE-2019-11599 instead of this candidate. A in this candidate have been removed to prevent accidental usage.
CVE-2014-8559	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The d_walk function in fs/dcache.c in the Linux kernel through 3.17.2 does not properly maintain the semanti allows local users to cause a denial of service (deadlock and system hang) via a crafted application.
CVE-2014-8559	perf-3.10.0-1127.13.1.el7.x86_64	perf	The d_walk function in fs/dcache.c in the Linux kernel through 3.17.2 does not properly maintain the semanti allows local users to cause a denial of service (deadlock and system hang) via a crafted application.
CVE-2014-8989	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The Linux kernel through 3.17.4 does not properly restrict dropping of supplemental group memberships in c which allows local users to bypass intended file permissions by leveraging a POSIX ACL containing an entry more restrictive than the entry for the other category, aka a "negative groups" issue, related to kernel/groups kernel/user_namespace.c.
CVE-2014-8989	perf-3.10.0-1127.13.1.el7.x86_64	perf	The Linux kernel through 3.17.4 does not properly restrict dropping of supplemental group memberships in c which allows local users to bypass intended file permissions by leveraging a POSIX ACL containing an entry more restrictive than the entry for the other category, aka a "negative groups" issue, related to kernel/groups kernel/user_namespace.c.
CVE-2016-9588	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest.
CVE-2016-9588	perf-3.10.0-1127.13.1.el7.x86_64	perf	arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest.
CVE-2014-7970	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The pivot_root implementation in fs/namespace.c in the Linux kernel through 3.17 does not properly interact chroot directory, which allows local users to cause a denial of service (mount-tree loop) via . (dot) values in b system call.
CVE-2014-7970	perf-3.10.0-1127.13.1.el7.x86_64	perf	The pivot_root implementation in fs/namespace.c in the Linux kernel through 3.17 does not properly interact chroot directory, which allows local users to cause a denial of service (mount-tree loop) via . (dot) values in b system call.
CVE-2014-0155	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ioapic_deliver function in virt/kvm/ioapic.c in the Linux kernel through 3.14.1 does not properly validate t return value, which allows guest OS users to cause a denial of service (host OS crash) via a crafted entry in APIC. NOTE: the affected code was moved to the ioapic_service function before the vulnerability was annou
CVE-2014-0155	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ioapic_deliver function in virt/kvm/ioapic.c in the Linux kernel through 3.14.1 does not properly validate t return value, which allows guest OS users to cause a denial of service (host OS crash) via a crafted entry in APIC. NOTE: the affected code was moved to the ioapic_service function before the vulnerability was annou

CVE-2019-14901	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	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 WiF allows a remote attacker to cause a system crash, resulting in a denial of service, or execute arbitrary code. vulnerability is with the availability of the system. If code execution occurs, the code will run with the permissi confidentiality and integrity of files on the system.
CVE-2019-14901	perf-3.10.0-1127.13.1.el7.x86_64	perf	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 WiF allows a remote attacker to cause a system crash, resulting in a denial of service, or execute arbitrary code. vulnerability is with the availability of the system. If code execution occurs, the code will run with the permissi confidentiality and integrity of files on the system.
CVE-2013-7266	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The mISDN_sock_recvmsg function in drivers/isdn/mISDN/socket.c in the Linux kernel before 3.12.4 does n value is consistent with the size of an associated data structure, which allows local users to obtain sensitive i via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2013-7266	perf-3.10.0-1127.13.1.el7.x86_64	perf	The mISDN_sock_recvmsg function in drivers/isdn/mISDN/socket.c in the Linux kernel before 3.12.4 does n value is consistent with the size of an associated data structure, which allows local users to obtain sensitive i via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2017-7533	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain pri service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_ha functions.
CVE-2017-7533	perf-3.10.0-1127.13.1.el7.x86_64	perf	Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain pri service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_ha functions.
CVE-2014-0049	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Buffer overflow in the complete_emulated_mmio function in arch/x86/kvm/x86.c in the Linux kernel before 3. execute arbitrary code on the host OS by leveraging a loop that triggers an invalid memory copy affecting ce
CVE-2014-0049	perf-3.10.0-1127.13.1.el7.x86_64	perf	Buffer overflow in the complete_emulated_mmio function in arch/x86/kvm/x86.c in the Linux kernel before 3. execute arbitrary code on the host OS by leveraging a loop that triggers an invalid memory copy affecting ce
CVE-2016-8646	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The hash_accept function in crypto/algif_hash.c in the Linux kernel before 4.3.6 allows local users to cause a attempting to trigger use of in-kernel hash algorithms for a socket that has received zero bytes of data.
CVE-2016-8646	perf-3.10.0-1127.13.1.el7.x86_64	perf	The hash_accept function in crypto/algif_hash.c in the Linux kernel before 4.3.6 allows local users to cause a attempting to trigger use of in-kernel hash algorithms for a socket that has received zero bytes of data.
CVE-2018-14625	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the Linux Kernel where an attacker may be able to have an uncontrolled read to kernel-m A race condition between connect() and close() function may allow an attacker using the AF_VSOCK protoco leak or possibly intercept or corrupt AF_VSOCK messages destined to other clients.
CVE-2018-14625	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the Linux Kernel where an attacker may be able to have an uncontrolled read to kernel-m A race condition between connect() and close() function may allow an attacker using the AF_VSOCK protoco leak or possibly intercept or corrupt AF_VSOCK messages destined to other clients.
CVE-2016-4794	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Use-after-free vulnerability in mm/percpu.c in the Linux kernel through 4.6 allows local users to cause a denia have unspecified other impact via crafted use of the mmap and bpf system calls.
CVE-2016-4794	perf-3.10.0-1127.13.1.el7.x86_64	perf	Use-after-free vulnerability in mm/percpu.c in the Linux kernel through 4.6 allows local users to cause a denia have unspecified other impact via crafted use of the mmap and bpf system calls.
CVE-2013-4579	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	The ath9k_htc_set_bssid_mask function in drivers/net/wireless/ath/ath9k/htc_drv_main.c in the Linux kernel masking approach to determine the set of MAC addresses on which a Wi-Fi device is listening, which allows the original MAC address after spoofing by sending a series of packets to MAC addresses with certain bit ma
CVE-2013-4579	perf-3.10.0-1127.13.1.el7.x86_64	perf	The ath9k_htc_set_bssid_mask function in drivers/net/wireless/ath/ath9k/htc_drv_main.c in the Linux kernel masking approach to determine the set of MAC addresses on which a Wi-Fi device is listening, which allows the original MAC address after spoofing by sending a series of packets to MAC addresses with certain bit ma
CVE-2016-5412	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	arch/powerpc/kvm/book3s_hv_rmhandlers.S in the Linux kernel through 4.7 on PowerPC platforms, when C is enabled, allows guest OS users to cause a denial of service (host OS infinite loop) by making a H_CEDE a suspended transaction.
CVE-2016-5412	perf-3.10.0-1127.13.1.el7.x86_64	perf	arch/powerpc/kvm/book3s_hv_rmhandlers.S in the Linux kernel through 4.7 on PowerPC platforms, when C is enabled, allows guest OS users to cause a denial of service (host OS infinite loop) by making a H_CEDE a suspended transaction.
CVE-2014-0131	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	Use-after-free vulnerability in the skb_segment function in net/core/skbuff.c in the Linux kernel through 3.13. sensitive information from kernel memory by leveraging the absence of a certain orphaning operation.
CVE-2014-0131	perf-3.10.0-1127.13.1.el7.x86_64	perf	Use-after-free vulnerability in the skb_segment function in net/core/skbuff.c in the Linux kernel through 3.13. sensitive information from kernel memory by leveraging the absence of a certain orphaning operation.
CVE-2019-10207	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A flaw was found in the Linux kernel's Bluetooth implementation of UART, all versions kernel 3.x.x before 4.1 attacker with local access and write permissions to the Bluetooth hardware could use this flaw to issue a spe and cause the system to crash.
CVE-2019-10207	perf-3.10.0-1127.13.1.el7.x86_64	perf	A flaw was found in the Linux kernel's Bluetooth implementation of UART, all versions kernel 3.x.x before 4.1 attacker with local access and write permissions to the Bluetooth hardware could use this flaw to issue a spe and cause the system to crash.

CVE-2017-7558	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	A kernel data leak due to an out-of-bound read was found in the Linux kernel in inet_diag_msg_sctp Unknown macro: {,l} addr_fill() and sctp_get_sctp_info() functions present since version 4.7-rc1 through version 4.13. A data leak fill in sockaddr data structures used to export socket's diagnostic information. As a result, up to 100 bytes of a userspace. | <table><tr><td>CVE-2017-7558</td><td>perf-3.10.0-1127.13.1.el7.x86_64</td><td>perf</td><td>A rea ine</td></tr></table> addr_fill() and sctp_get_sctp_info() functions present since version 4.7-rc1 through version 4.13. A data leak fill in sockaddr data structures used to export socket's diagnostic information. As a result, up to 100 bytes of a userspace.
CVE-2019-13233	kernel-3.10.0-1127.13.1.el7.x86_64	kernel	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 between modify_ldt() and a #BR exception for an MPX bounds violation.
CVE-2019-13233	perf-3.10.0-1127.13.1.el7.x86_64	perf	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 between modify_ldt() and a #BR exception for an MPX bounds violation.
CVE-2018-18311	perl-5.16.3-294.el7_6.x86_64	perl	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that trigger
CVE-2018-18311	perl-Pod-Escapes-1.04-294.el7_6.noarch	perl-Pod-Escapes	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that trigger
CVE-2018-18311	perl-libs-5.16.3-294.el7_6.x86_64	perl-libs	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that trigger
CVE-2011-3597	perl-5.16.3-294.el7_6.x86_64	perl	Eval injection vulnerability in the Digest module before 1.17 for Perl allows context-dependent attackers to ex the new constructor.
CVE-2011-3597	perl-Pod-Escapes-1.04-294.el7_6.noarch	perl-Pod-Escapes	Eval injection vulnerability in the Digest module before 1.17 for Perl allows context-dependent attackers to ex the new constructor.
CVE-2011-3597	perl-libs-5.16.3-294.el7_6.x86_64	perl-libs	Eval injection vulnerability in the Digest module before 1.17 for Perl allows context-dependent attackers to ex the new constructor.
CVE-2011-2728	perl-5.16.3-294.el7_6.x86_64	perl	The bsd_glob function in the File::Glob module for Perl before 5.14.2 allows context-dependent attackers to (crash) via a glob expression with the GLOB_ALTDIRFUNC flag, which triggers an uninitialized pointer deref
CVE-2011-2728	perl-Pod-Escapes-1.04-294.el7_6.noarch	perl-Pod-Escapes	The bsd_glob function in the File::Glob module for Perl before 5.14.2 allows context-dependent attackers to (crash) via a glob expression with the GLOB_ALTDIRFUNC flag, which triggers an uninitialized pointer deref
CVE-2011-2728	perl-libs-5.16.3-294.el7_6.x86_64	perl-libs	The bsd_glob function in the File::Glob module for Perl before 5.14.2 allows context-dependent attackers to (crash) via a glob expression with the GLOB_ALTDIRFUNC flag, which triggers an uninitialized pointer deref
CVE-2014-2524	readline-6.2-11.el7.x86_64	readline	The _rl_tropen function in util.c in GNU readline before 6.3 patch 3 allows local users to create or overwrite a attack on a /var/tmp/rltrace.PID file.
CVE-2016-2183	python-2.7.5-86.el7.x86_64	python	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSecprotocols and other protocols and pro approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birt long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka
CVE-2016-2183	python-libs-2.7.5-86.el7.x86_64	python-libs	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSecprotocols and other protocols and pro approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birt long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka
CVE-2019-9740	python-2.7.5-86.el7.x86_64	python	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (sp after a ? character) followed by an HTTP header or a Redis command.
CVE-2019-9740	python-libs-2.7.5-86.el7.x86_64	python-libs	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (sp after a ? character) followed by an HTTP header or a Redis command.
CVE-2019-9948	python-2.7.5-86.el7.x86_64	python	urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_ file:///etc/passwd ') call.
CVE-2019-9948	python-libs-2.7.5-86.el7.x86_64	python-libs	urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_ file:///etc/passwd ') call.
CVE-2018-14647	python-2.7.5-86.el7.x86_64	python	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make i service attacks against Expat by constructing an XML document that would cause pathological hash collisior structures, consuming large amounts CPU and RAM. The vulnerability exists in Python versions 3.7.0, 3.6.0 3.5.6, 3.4.0 through 3.4.9, 2.7.0 through 2.7.15.
CVE-2018-14647	python-libs-2.7.5-86.el7.x86_64	python-libs	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make i service attacks against Expat by constructing an XML document that would cause pathological hash collisior structures, consuming large amounts CPU and RAM. The vulnerability exists in Python versions 3.7.0, 3.6.0 3.5.6, 3.4.0 through 3.4.9, 2.7.0 through 2.7.15.

CVE-2014-4616	python-2.7.5-86.el7.x86_64	python	Array index error in the scanstring function in the _json module in Python 2.7 through 3.5 and simplejson bef context-dependent attackers to read arbitrary process memory via a negative index value in the idx argumen
CVE-2014-4616	python-libs-2.7.5-86.el7.x86_64	python-libs	Array index error in the scanstring function in the _json module in Python 2.7 through 3.5 and simplejson bef context-dependent attackers to read arbitrary process memory via a negative index value in the idx argumen
CVE-2018-1060	python-2.7.5-86.el7.x86_64	python	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking i attacker could use this flaw to cause denial of service.
CVE-2018-1060	python-libs-2.7.5-86.el7.x86_64	python-libs	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking i attacker could use this flaw to cause denial of service.
CVE-2019-9947	python-2.7.5-86.el7.x86_64	python	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (sp of a URL that lacks a ? character) followed by an HTTP header or a Redis command. This is similar to the C issue.
CVE-2019-9947	python-libs-2.7.5-86.el7.x86_64	python-libs	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (sp of a URL that lacks a ? character) followed by an HTTP header or a Redis command. This is similar to the C issue.
CVE-2014-4650	python-2.7.5-86.el7.x86_64	python	The CGIHTTPServer module in Python 2.7.5 and 3.3.4 does not properly handle URLs in which URL encodi which allows remote attackers to read script source code or conduct directory traversal attacks and execute character sequence, as demonstrated by a %2f separator.
CVE-2014-4650	python-libs-2.7.5-86.el7.x86_64	python-libs	The CGIHTTPServer module in Python 2.7.5 and 3.3.4 does not properly handle URLs in which URL encodi which allows remote attackers to read script source code or conduct directory traversal attacks and execute character sequence, as demonstrated by a %2f separator.
CVE-2013-1753	python-2.7.5-86.el7.x86_64	python	The gzip_decode function in the xmlrpc client library in Python 3.4 and earlier allows remote attackers to cau consumption) via a crafted HTTP request.
CVE-2013-1753	python-libs-2.7.5-86.el7.x86_64	python-libs	The gzip_decode function in the xmlrpc client library in Python 3.4 and earlier allows remote attackers to cau consumption) via a crafted HTTP request.
CVE-2019-5010	python-2.7.5-86.el7.x86_64	python	An exploitable denial-of-service vulnerability exists in the X509 certificate parser of Python.org Python 2.7.11 X509 certificate can cause a NULL pointer dereference, resulting in a denial of service. An attacker can initia using crafted certificates to trigger this vulnerability.
CVE-2019-5010	python-libs-2.7.5-86.el7.x86_64	python-libs	An exploitable denial-of-service vulnerability exists in the X509 certificate parser of Python.org Python 2.7.11 X509 certificate can cause a NULL pointer dereference, resulting in a denial of service. An attacker can initia using crafted certificates to trigger this vulnerability.
CVE-2018-1061	python-2.7.5-86.el7.x86_64	python	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking i method. An attacker could use this flaw to cause denial of service.
CVE-2018-1061	python-libs-2.7.5-86.el7.x86_64	python-libs	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking i method. An attacker could use this flaw to cause denial of service.
CVE-2016-5636	python-2.7.5-86.el7.x86_64	python	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-bas
CVE-2016-5636	python-libs-2.7.5-86.el7.x86_64	python-libs	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-bas
CVE-2014-8118	rpm-4.11.3-40.el7.x86_64	rpm	Integer overflow in RPM 4.12 and earlier allows remote attackers to execute arbitrary code via a crafted CPI of an RPM file, which triggers a stack-based buffer overflow.
CVE-2014-8118	rpm-libs-4.11.3-40.el7.x86_64	rpm-libs	Integer overflow in RPM 4.12 and earlier allows remote attackers to execute arbitrary code via a crafted CPI of an RPM file, which triggers a stack-based buffer overflow.
CVE-2014-8118	rpm-python-4.11.3-40.el7.x86_64	rpm-python	Integer overflow in RPM 4.12 and earlier allows remote attackers to execute arbitrary code via a crafted CPI of an RPM file, which triggers a stack-based buffer overflow.
CVE-2013-2131	rrdtool-1.4.8-9.el7.x86_64	rrdtool	Format string vulnerability in the rrdtool module 1.4.7 for Python, as used in Zenoss, allows context-depende of service (crash) via format string specifiers to the rrdtool.graph function.
CVE-2013-2131	rrdtool-perl-1.4.8-9.el7.x86_64	rrdtool-perl	Format string vulnerability in the rrdtool module 1.4.7 for Python, as used in Zenoss, allows context-depende of service (crash) via format string specifiers to the rrdtool.graph function.
CVE-2018-16881	rsyslog-8.24.0-52.el7_8.2.x86_64	rsyslog	A denial of service vulnerability was found in rsyslog in the imptcp module. An attacker could send a specially socket, which would cause rsyslog to crash. Versions before 8.27.0 are vulnerable.
CVE-2016-2119	samba-4.9.1-6.el7.x86_64	samba	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 mar 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.
CVE-2016-2119	samba-common-4.9.1-6.el7.noarch	samba-common	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 mar 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.
CVE-2016-2119	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	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 mar 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.

CVE-2016-2119	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	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 mar 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.
CVE-2014-0178	samba-4.9.1-6.el7.x86_64	samba	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 cor properly initialize the SRV_SNAPSHOT_ARRAY response field, which allows remote authenticated users to information from process memory via a (1) FSCTL_GET_SHADOW_COPY_DATA or (2) FSCTL_SRV_ENU request.
CVE-2014-0178	samba-common-4.9.1-6.el7.noarch	samba-common	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 cor properly initialize the SRV_SNAPSHOT_ARRAY response field, which allows remote authenticated users to information from process memory via a (1) FSCTL_GET_SHADOW_COPY_DATA or (2) FSCTL_SRV_ENU request.
CVE-2014-0178	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	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 cor properly initialize the SRV_SNAPSHOT_ARRAY response field, which allows remote authenticated users to information from process memory via a (1) FSCTL_GET_SHADOW_COPY_DATA or (2) FSCTL_SRV_ENU request.
CVE-2014-0178	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	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 cor properly initialize the SRV_SNAPSHOT_ARRAY response field, which allows remote authenticated users to information from process memory via a (1) FSCTL_GET_SHADOW_COPY_DATA or (2) FSCTL_SRV_ENU request.
CVE-2012-0817	samba-4.9.1-6.el7.x86_64	samba	Memory leak in smbd in Samba 3.6.x before 3.6.3 allows remote attackers to cause a denial of service (mem making many connection requests.
CVE-2012-0817	samba-common-4.9.1-6.el7.noarch	samba-common	Memory leak in smbd in Samba 3.6.x before 3.6.3 allows remote attackers to cause a denial of service (mem making many connection requests.
CVE-2012-0817	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	Memory leak in smbd in Samba 3.6.x before 3.6.3 allows remote attackers to cause a denial of service (mem making many connection requests.
CVE-2012-0817	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	Memory leak in smbd in Samba 3.6.x before 3.6.3 allows remote attackers to cause a denial of service (mem making many connection requests.
CVE-2018-1139	samba-4.9.1-6.el7.x86_64	samba	A flaw was found in the way samba before 4.7.9 and 4.8.4 allowed the use of weak NTLMv1 authentication e explicitly disabled. A man-in-the-middle attacker could use this flaw to read the credential and other details p server and client.
CVE-2018-1139	samba-common-4.9.1-6.el7.noarch	samba-common	A flaw was found in the way samba before 4.7.9 and 4.8.4 allowed the use of weak NTLMv1 authentication e explicitly disabled. A man-in-the-middle attacker could use this flaw to read the credential and other details p server and client.
CVE-2018-1139	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	A flaw was found in the way samba before 4.7.9 and 4.8.4 allowed the use of weak NTLMv1 authentication e explicitly disabled. A man-in-the-middle attacker could use this flaw to read the credential and other details p server and client.
CVE-2018-1139	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	A flaw was found in the way samba before 4.7.9 and 4.8.4 allowed the use of weak NTLMv1 authentication e explicitly disabled. A man-in-the-middle attacker could use this flaw to read the credential and other details p server and client.
CVE-2017-14746	samba-4.9.1-6.el7.x86_64	samba	Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a
CVE-2017-14746	samba-common-4.9.1-6.el7.noarch	samba-common	Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a
CVE-2017-14746	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a
CVE-2017-14746	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a
CVE-2018-10858	samba-4.9.1-6.el7.x86_64	samba	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listin could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9
CVE-2018-10858	samba-common-4.9.1-6.el7.noarch	samba-common	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listin could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9
CVE-2018-10858	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listin could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9
CVE-2018-10858	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listin could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9
CVE-2017-15275	samba-4.9.1-6.el7.x86_64	samba	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the s memory.
CVE-2017-15275	samba-common-4.9.1-6.el7.noarch	samba-common	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the s memory.
CVE-2017-15275	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the s memory.
CVE-2017-15275	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the s memory.
CVE-2013-0172	samba-4.9.1-6.el7.x86_64	samba	Samba 4.0.x before 4.0.1, in certain Active Directory domain-controller configurations, does not properly inte that are based on an objectClass, which allows remote authenticated users to bypass intended restrictions o objects by leveraging (1) objectClass access by a user, (2) objectClass access by a group, or (3) write acces

CVE-2013-0172	samba-common-4.9.1-6.el7.noarch	samba-common	Samba 4.0.x before 4.0.1, in certain Active Directory domain-controller configurations, does not properly inte that are based on an objectClass, which allows remote authenticated users to bypass intended restrictions o objects by leveraging (1) objectClass access by a user, (2) objectClass access by a group, or (3) write acces
CVE-2013-0172	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	Samba 4.0.x before 4.0.1, in certain Active Directory domain-controller configurations, does not properly inte that are based on an objectClass, which allows remote authenticated users to bypass intended restrictions o objects by leveraging (1) objectClass access by a user, (2) objectClass access by a group, or (3) write acces
CVE-2013-0172	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	Samba 4.0.x before 4.0.1, in certain Active Directory domain-controller configurations, does not properly inte that are based on an objectClass, which allows remote authenticated users to bypass intended restrictions o objects by leveraging (1) objectClass access by a user, (2) objectClass access by a group, or (3) write acces
CVE-2016-2113	samba-4.9.1-6.el7.x86_64	samba	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 TL man-in-the-middle attackers to spoof LDAPS and HTTPS servers and obtain sensitive information via a craft
CVE-2016-2113	samba-common-4.9.1-6.el7.noarch	samba-common	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 TL man-in-the-middle attackers to spoof LDAPS and HTTPS servers and obtain sensitive information via a craft
CVE-2016-2113	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	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 TL man-in-the-middle attackers to spoof LDAPS and HTTPS servers and obtain sensitive information via a craft
CVE-2016-2113	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	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 TL man-in-the-middle attackers to spoof LDAPS and HTTPS servers and obtain sensitive information via a craft
CVE-2019-3880	samba-4.9.1-6.el7.x86_64	samba	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service A could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead t Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
CVE-2019-3880	samba-common-4.9.1-6.el7.noarch	samba-common	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service A could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead t Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
CVE-2019-3880	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service A could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead t Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
CVE-2019-3880	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service A could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead t Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
CVE-2016-2114	samba-4.9.1-6.el7.x86_64	samba	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 do signing = mandatory" setting, which allows man-in-the-middle attackers to spoof SMB servers by modifying t
CVE-2016-2114	samba-common-4.9.1-6.el7.noarch	samba-common	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 do signing = mandatory" setting, which allows man-in-the-middle attackers to spoof SMB servers by modifying t
CVE-2016-2114	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	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 do signing = mandatory" setting, which allows man-in-the-middle attackers to spoof SMB servers by modifying t
CVE-2016-2114	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	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 do signing = mandatory" setting, which allows man-in-the-middle attackers to spoof SMB servers by modifying t
CVE-2015-3223	samba-4.9.1-6.el7.x86_64	samba	The ldb_wildcard_compare function in ldb_match.c in ldb before 1.1.24, as used in the AD LDAP server in S before 4.2.7, and 4.3.x before 4.3.3, mishandles certain zero values, which allows remote attackers to cause loop) via crafted packets.
CVE-2015-3223	samba-common-4.9.1-6.el7.noarch	samba-common	The ldb_wildcard_compare function in ldb_match.c in ldb before 1.1.24, as used in the AD LDAP server in S before 4.2.7, and 4.3.x before 4.3.3, mishandles certain zero values, which allows remote attackers to cause loop) via crafted packets.
CVE-2015-3223	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	The ldb_wildcard_compare function in ldb_match.c in ldb before 1.1.24, as used in the AD LDAP server in S before 4.2.7, and 4.3.x before 4.3.3, mishandles certain zero values, which allows remote attackers to cause loop) via crafted packets.
CVE-2015-3223	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	The ldb_wildcard_compare function in ldb_match.c in ldb before 1.1.24, as used in the AD LDAP server in S before 4.2.7, and 4.3.x before 4.3.3, mishandles certain zero values, which allows remote attackers to cause loop) via crafted packets.
CVE-2017-12151	samba-4.9.1-6.el7.x86_64	samba	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encrypt as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowi the contents of the connection via a man-in-the-middle attack.
CVE-2017-12151	samba-common-4.9.1-6.el7.noarch	samba-common	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encrypt as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowi the contents of the connection via a man-in-the-middle attack.
CVE-2017-12151	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encrypt as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowi the contents of the connection via a man-in-the-middle attack.
CVE-2017-12151	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encrypt as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowi the contents of the connection via a man-in-the-middle attack.
CVE-2014-3560	samba-4.9.1-6.el7.x86_64	samba	NetBIOS name services daemon (nmbd) in Samba 4.0.x before 4.0.21 and 4.1.x before 4.1.11 allows remote code via unspecified vectors that modify heap memory, involving a sizeof operation on an incorrect variable i string_wrappers.h.

CVE-2014-3560	samba-common-4.9.1-6.el7.noarch	samba-common	NetBIOS name services daemon (nmbd) in Samba 4.0.x before 4.0.21 and 4.1.x before 4.1.11 allows remote code via unspecified vectors that modify heap memory, involving a sizeof operation on an incorrect variable i string_wrappers.h.
CVE-2014-3560	samba-winbind-4.9.1-6.el7.x86_64	samba-winbind	NetBIOS name services daemon (nmbd) in Samba 4.0.x before 4.0.21 and 4.1.x before 4.1.11 allows remote code via unspecified vectors that modify heap memory, involving a sizeof operation on an incorrect variable i string_wrappers.h.
CVE-2014-3560	samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients	NetBIOS name services daemon (nmbd) in Samba 4.0.x before 4.0.21 and 4.1.x before 4.1.11 allows remote code via unspecified vectors that modify heap memory, involving a sizeof operation on an incorrect variable i string_wrappers.h.
CVE-2015-3415	sqlite-3.7.17-8.el7.x86_64	sqlite	The sqlite3VdbeExec function in vdbe.c in SQLite before 3.8.9 does not properly implement comparison ope context-dependent attackers to cause a denial of service (invalid free operation) or possibly have unspecifiec CHECK clause, as demonstrated by CHECK(0&O>O) in a CREATE TABLE statement.
CVE-2015-3414	sqlite-3.7.17-8.el7.x86_64	sqlite	SQLite before 3.8.9 does not properly implement the dequoting of collation-sequence names, which allows c cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified o COLLATE clause, as demonstrated by COLLATE""""""""""""" at the end of a SELECT statement.
CVE-2008-5110	syslog-ng-3.5.6-3.el7.x86_64	syslog-ng	syslog-ng does not call chdir when it calls chroot, which might allow attackers to escape the intended jail. NC when a separate vulnerability is present.
CVE-2012-0809	sudo-1.8.23-9.el7.x86_64	sudo	Format string vulnerability in the sudo_debug function in Sudo 1.8.0 through 1.8.3p1 allows local users to ex string sequences in the program name for sudo.
CVE-2011-0010	sudo-1.8.23-9.el7.x86_64	sudo	check.c in sudo 1.7.x before 1.7.4p5, when a Runas group is configured, does not require a password for co a gid change but no uid change, which allows local users to bypass an intended authentication requirement v command.
CVE-2011-0008	sudo-1.8.23-9.el7.x86_64	sudo	A certain Fedora patch for parse.c in sudo before 1.7.4p5-1.fc14 on Fedora 14 does not properly interpret a s the sudoers file during authorization decisions for a user who belongs to that group, which allows local users sudoers file and gain root privileges via a sudo command. NOTE: this vulnerability exists because of a CVE-
CVE-2013-1776	sudo-1.8.23-9.el7.x86_64	sudo	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 device, which allows local users with sudo permissions to hijack the authorization of another terminal via vec standard input, output, and error file descriptors of another terminal. NOTE: this is one of three closely-relate originally assigned CVE-2013-1776, but they have been SPLIT because of different affected versions.
CVE-2018-18384	unzip-6.0-20.el7.x86_64	unzip	Info-ZIP UnZip 6.0 has a buffer overflow in list.c, when a ZIP archive has a crafted relationship between the uncompressed-size value, because a buffer size is 10 and is supposed to be 12.

Packages updated for Security reasons.

Old Package	New Package for CVE
java-1.8.0-openjdk-headless-1.8.0.232.b09-1.el6_10.x86_64	java-1.8.0-openjdk-headless-1.8.0.242.b07-1.el6_10.x86_64
kernel-2.6.32-754.23.1.el6.x86_64	kernel-2.6.32-754.28.1.el6.x86_64
kernel-firmware-2.6.32-754.23.1.el6.noarch	kernel-firmware-2.6.32-754.28.1.el6.noarch
kernel-headers-2.6.32-754.23.1.el6.x86_64	kernel-headers-2.6.32-754.28.1.el6.x86_64
nspr-4.19.0-1.el6.x86_64	nspr-4.21.0-1.el6_10.x86_64
nss-3.36.0-9.el6_10.x86_64	nss-3.44.0-7.el6_10.x86_64
nss-softokn-3.14.3-23.3.el6_8.x86_64	nss-softokn-3.44.0-6.el6_10.x86_64
nss-softokn-freebl-3.14.3-23.3.el6_8.x86_64	nss-softokn-freebl-3.44.0-6.el6_10.x86_64
nss-sysinit-3.36.0-9.el6_10.x86_64	nss-sysinit-3.44.0-7.el6_10.x86_64
nss-tools-3.36.0-9.el6_10.x86_64	nss-tools-3.44.0-7.el6_10.x86_64
nss-util-3.36.0-1.el6.x86_64	nss-util-3.44.0-1.el6_10.x86_64

openssh-5.3p1-123.el6_9.x86_64	openssh-5.3p1-124.el6_10.x86_64
openssh-clients-5.3p1-123.el6_9.x86_64	openssh-clients-5.3p1-124.el6_10.x86_64
openssh-server-5.3p1-123.el6_9.x86_64	openssh-server-5.3p1-124.el6_10.x86_64
perf-2.6.32-754.23.1.el6.x86_64	perf-2.6.32-754.28.1.el6.x86_64
sudo-1.8.6p3-29.el6_9.x86_64	sudo-1.8.6p3-29.el6_10.3.x86_64

Packages updated NOT for Security reasons.

Old Package	New Package NOT for CVE
esi-release-3.3.4.0-28733.3850.x86_64	esi-release-3.3.5.0-30536.4285.x86_64
logbase-ui-3.3.4.0-20191114200425.x86_64	logbase-ui-3.3.5.0-20200409092507.x86_64
lumeta-api-3.3.4.0-28726.x86_64	lumeta-api-3.3.5.0-30535.x86_64
lumeta-api-client-3.3.4.0-13896.x86_64	lumeta-api-client-3.3.5.0-29193.x86_64
lumeta-cisco-ise-pxgrid-3.3.3.0-12060.x86_64	lumeta-cisco-ise-pxgrid-3.3.4.1-26411.x86_64
lumeta-console-3.3.4.0-28504.x86_64	lumeta-console-3.3.5.0-30234.x86_64
lumeta-diagnostics-3.3.4.0-28671.x86_64	lumeta-diagnostics-3.3.5.0-30488.x86_64
lumeta-discovery-agent-3.3.4.0-28675.x86_64	lumeta-discovery-agent-3.3.5.0-30519.x86_64
lumeta-dxl-3.3.4.0-13229.x86_64	lumeta-dxl-3.3.5.0-13229.x86_64
lumeta-install-3.3.4.0-28732.x86_64	lumeta-install-3.3.5.0-30460.x86_64
lumeta-ips-import-3.3.3.0-6550.x86_64	lumeta-ips-import-3.3.4.1-6550.x86_64
lumeta-ireg-3.3.4.0-6550.x86_64	lumeta-ireg-3.3.5.0-6550.x86_64
lumeta-jaas-3.3.3.0-13398.x86_64	lumeta-jaas-3.3.5.0-13398.x86_64
lumeta-lib-3.3.4.0-28641.x86_64	lumeta-lib-3.3.5.0-29992.x86_64
lumeta-pam-3.3.4.0-18946.x86_64	lumeta-pam-3.3.5.0-30422.x86_64
lumeta-tfa-3.3.3.0-10659.x86_64	lumeta-tfa-3.3.4.1-10659.x86_64
lumeta-tools-3.3.3.0-10695.x86_64	lumeta-tools-3.3.4.1-10695.x86_64
lumeta-ui-3.3.4.0-28464.x86_64	lumeta-ui-3.3.5.0-30195.x86_64

lumeta-visio-3.3.3.0-12259.x86_64	lumeta-visio-3.3.4.1-12259.x86_64
lumeta-webapp-3.3.4.0-13900.x86_64	lumeta-webapp-3.3.4.1-13900.x86_64
rawio-3.3.3.0-8288.x86_64	rawio-3.3.4.1-8288.x86_64
x15-backend-3.3.4.0-13991.x86_64	x15-backend-3.3.4.1-13991.x86_64

New packages.