Security Advisories 4.3

This page shows the package changes from 4.2 to 4.3 some for security reasons and the CVEs.

Deliverable	Name
upgrade	lumeta_update-4.3.0.0.35578-20210908.tgz

CVEs and the new package and RPM that resolves each

CVE	New RPM	PKG	DESCRIPTION
CVE-2020-12049	dbus-1.10.24-15.el7.x86_64	dbus	An issue was discovered in dbus >= 1.3.0 before 1.12.18. The DBusServer in libdbus, as used in dbus-daemon, leaks file descriptors when a message exceeds the per-message file descriptor limit. A local attacker with access to the D-Bus system bus or another system service's private AF_UNIX socket could use this to make the system service reach its file descriptor limit, denying service to subsequent D-Bus clients.
CVE-2020-12049	dbus-libs-1.10.24-15.el7.x86_64	dbus-libs	An issue was discovered in dbus >= 1.3.0 before 1.12.18. The DBusServer in libdbus, as used in dbus-daemon, leaks file descriptors when a message exceeds the per-message file descriptor limit. A local attacker with access to the D-Bus system bus or another system service's private AF_UNIX socket could use this to make the system service reach its file descriptor limit, denying service to subsequent D-Bus clients.
CVE-2019-12749	dbus-1.10.24-15.el7.x86_64	dbus	dbus before 1.10.28, 1.12.x before 1.12.16, and 1.13.x before 1.13.12, as used in DBusServer in Canonical Upstart in Ubuntu 14.04 (and in some, less common, uses of dbus-daemon), allows cookie spoofing because of symlink mishandling in the reference implementation of DBUS_COOKIE_SHA1 in the libdbus library. (This only affects the DBUS_COOKIE_SHA1 authentication mechanism.) A malicious client with write access to its own home directory could manipulate a ~/.dbus-keyrings symlink to cause a DBusServer with a different uid to read and write in unintended locations. In the worst case, this could result in the DBusServer reusing a cookie that is known to the malicious client, and treating that cookie as evidence that a subsequent client connection came from an attacker-chosen uid, allowing authentication bypass.
CVE-2019-12749	dbus-libs-1.10.24-15.el7.x86_64	dbus-libs	dbus before 1.10.28, 1.12.x before 1.12.16, and 1.13.x before 1.13.12, as used in DBusServer in Canonical Upstart in Ubuntu 14.04 (and in some, less common, uses of dbus-daemon), allows cookie spoofing because of symlink mishandling in the reference implementation of DBUS_COOKIE_SHA1 in the libdbus library. (This only affects the DBUS_COOKIE_SHA1 authentication mechanism.) A malicious client with write access to its own home directory could manipulate a ~/.dbus-keyrings symlink to cause a DBusServer with a different uid to read and write in unintended locations. In the worst case, this could result in the DBusServer reusing a cookie that is known to the malicious client, and treating that cookie as evidence that a subsequent client connection came from an attacker-chosen uid, allowing authentication bypass.
CVE-2020-10754	NetworkManager-1.18.8-2.el7_9.x86_64	Network Manager	It was found that nmcli, a command line interface to NetworkManager did not honour 802-1x.ca-path and 802-1x.phase2-ca-path settings, when creating a new profile. When a user connects to a network using this profile, the authentication does not happen and the connection is made insecurely.
CVE-2020-10754	NetworkManager-libnm-1.18.8-2.el7_9.x86_64	Network Manager-libnm	It was found that nmcli, a command line interface to NetworkManager did not honour 802-1x.ca-path and 802-1x.phase2-ca-path settings, when creating a new profile. When a user connects to a network using this profile, the authentication does not happen and the connection is made insecurely.
CVE-2020-10754	NetworkManager-team-1.18.8-2.el7_9.x86_64	Network Manager-team	It was found that nmcli, a command line interface to NetworkManager did not honour 802-1x.ca-path and 802-1x.phase2-ca-path settings, when creating a new profile. When a user connects to a network using this profile, the authentication does not happen and the connection is made insecurely.
CVE-2020-10754	NetworkManager-tui-1.18.8-2.el7_9.x86_64	Network Manager-tui	It was found that nmcli, a command line interface to NetworkManager did not honour 802-1x.ca-path and 802-1x.phase2-ca-path settings, when creating a new profile. When a user connects to a network using this profile, the authentication does not happen and the connection is made insecurely.
CVE-2019-8675	cups-client-1.6.3-51.el7.x86_64	cups-client	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. An attacker in a privileged network position may be able to execute arbitrary code.
CVE-2019-8675	cups-libs-1.6.3-51.el7.x86_64	cups-libs	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. An attacker in a privileged network position may be able to execute arbitrary code.
CVE-2017-18190	cups-client-1.6.3-51.el7.x86_64	cups-client	A localhost.localdomain whitelist entry in valid_host() in scheduler/client.c in CUPS before 2.2.2 allows remote attackers to execute arbitrary IPP commands by sending POST requests to the CUPS daemon in conjunction with DNS rebinding. The localhost.localdomain name is often resolved via a DNS server (neither the OS nor the web browser is responsible for ensuring that localhost.localdomain is 127.0.0.1).
CVE-2017-18190	cups-libs-1.6.3-51.el7.x86_64	cups-libs	A localhost.localdomain whitelist entry in valid_host() in scheduler/client.c in CUPS before 2.2.2 allows remote attackers to execute arbitrary IPP commands by sending POST requests to the CUPS daemon in conjunction with DNS rebinding. The localhost.localdomain name is often resolved via a DNS server (neither the OS nor the web browser is responsible for ensuring that localhost.localdomain is 127.0.0.1).
CVE-2018-4181	cups-client-1.6.3-51.el7.x86_64	cups-client	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.
CVE-2018-4181	cups-libs-1.6.3-51.el7.x86_64	cups-libs	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.
CVE-2018-4700	cups-client-1.6.3-51.el7.x86_64	cups-client	• • DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-4300. Reason: This candidate is a duplicate of CVE-2018-4300. Notes: All CVE users should reference CVE-2018-4300 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2018-4700	cups-libs-1.6.3-51.el7.x86_64	cups-libs	• • DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2018-4300. Reason: This candidate is a duplicate of CVE-2018-4300. Notes: All CVE users should reference CVE-2018-4300 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.

CVE-2018-4180	cups-client-1.6.3-51.el7.x86_64	cups-client	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.
CVE-2018-4180	cups-libs-1.6.3-51.el7.x86_64	cups-libs	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.
CVE-2019-8696	cups-client-1.6.3-51.el7.x86_64	cups-client	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. An attacker in a privileged network position may be able to execute arbitrary code.
CVE-2019-8696	cups-libs-1.6.3-51.el7.x86_64	cups-libs	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. An attacker in a privileged network position may be able to execute arbitrary code.
CVE-2020-8177	curl-7.29.0-59.el7_9.1.x86_64	curl	curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of names for files and other resources that can lead too overwriting a local file when the -J flag is used.
CVE-2020-8177	libcurl-7.29.0-59.el7_9.1.x86_64	libcurl	curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of names for files and other resources that can lead too overwriting a local file when the -J flag is used.
CVE-2019-18397	fribidi-1.0.2-1.el7_7.1.x86_64	fribidi	A buffer overflow in the fribidi_get_par_embedding_levels_ex() function in lib/fribidi-bidi.c of GNU FriBidi through 1.0.7 allows an attacker to cause a denial of service or possibly execute arbitrary code by delivering crafted text content to a user, when this content is then rendered by an application that uses FriBidi for text layout calculations. Examples include any GNOME or GTK+ based application that uses Pango for text layout, as this internally uses FriBidi for bidirectional text layout. For example, the attacker can construct a crafted text file to be opened in GEdit, or a crafted IRC message to be viewed in HexChat.
CVE-2018-10360	file-5.11-37.el7.x86_64	file	The do_core_note function in readelf.c in libmagic.a in file 5.33 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted ELF file.
CVE-2018-10360	file-libs-5.11-37.el7.x86_64	file-libs	The do_core_note function in readelf.c in libmagic.a in file 5.33 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted ELF file.
CVE-2021-27219	glib2-2.56.1-9.el7_9.x86_64	glib2	An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before 2.67.3. The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.
CVE-2021-27219	glib2-devel-2.56.1-9.el7_9.x86_64	glib2-devel	An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before 2.67.3. The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.
CVE-2019-19126	glibc-2.17-323.el7_9.x86_64	glibc	On the x86-64 architecture, the GNU C Library (aka glibc) before 2.31 fails to ignore the LD_PREFER_MAP_32BIT_EXEC environment variable during program execution after a security transition, allowing local attackers to restrict the possible mapping addresses for loaded libraries and thus bypass ASLR for a setuid program.
CVE-2019-19126	glibc-common-2.17-323.el7_9.x86_64	glibc-common	On the x86-64 architecture, the GNU C Library (aka glibc) before 2.31 fails to ignore the LD_PREFER_MAP_32BIT_EXEC environment variable during program execution after a security transition, allowing local attackers to restrict the possible mapping addresses for loaded libraries and thus bypass ASLR for a setuid program.
CVE-2019-25013	glibc-2.17-323.el7_9.x86_64	glibc	The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.
CVE-2019-25013	glibc-common-2.17-323.el7_9.x86_64	glibc-common	The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.
CVE-2020-29573	glibc-2.17-323.el7_9.x86_64	glibc	sysdeps/i386/ldbl2mpn.c in the GNU C Library (aka glibc or libc6) before 2.23 on x86 targets has a stack-based buffer overflow if the input to any of the printf family of functions is an 80-bit long double with a non-canonical bit pattern, as seen when passing a \x00\x04\x00\x00\x00\x00\x00\x00\x00\x04 value to sprintf. NOTE: the issue does not affect glibc by default in 2016 or later (i.e., 2.23 or later) because of commits made in 2015 for inlining of C99 math functions through use of GCC built-ins. In other words, the reference to 2.23 is intentional despite the mention of "Fixed for glibc 2.33" in the 26649 reference.
CVE-2020-29573	glibc-common-2.17-323.el7_9.x86_64	glibc-common	sysdeps/i386/ldbl2mpn.c in the GNU C Library (aka glibc or libc6) before 2.23 on x86 targets has a stack-based buffer overflow if the input to any of the printf family of functions is an 80-bit long double with a non-canonical bit pattern, as seen when passing a \x00\x04\x00\x00\x00\x00\x00\x00\x00\x04 value to sprintf. NOTE: the issue does not affect glibc by default in 2016 or later (i.e., 2.23 or later) because of commits made in 2015 for inlining of C99 math functions through use of GCC built-ins. In other words, the reference to 2.23 is intentional despite the mention of "Fixed for glibc 2.33" in the 26649 reference.
CVE-2020-10029	glibc-2.17-323.el7_9.x86_64	glibc	The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d414141414141410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c.
CVE-2020-10029	glibc-common-2.17-323.el7_9.x86_64	glibc-common	The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, a seen when passing a 0x5d414141414141410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/ldbl-96/e_rem_pio2l.c.
CVE-2020-14310	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow.
CVE-2020-14310	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow.
CVE-2020-14310	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow.

CVE-2020-14310	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow.
CVE-2020-14310	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow.
CVE-2020-14310	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow.
CVE-2020-14310	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow.
CVE-2020-15705	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-15705	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-15705	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-15705	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-15705	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-15705	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-15705	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-14309	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data.
CVE-2020-14309	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data.
CVE-2020-14309	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data.
CVE-2020-14309	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data.
CVE-2020-14309	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data.

CVE-2020-14309	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data.
CVE-2020-14309	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data.
CVE-2021-20233	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20233	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20233	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20233	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20233	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20233	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20233	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25632	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25632	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25632	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25632	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25632	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25632	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25632	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-14372	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	A flaw was found in grub2 in versions prior to 2.06, where it incorrectly enables the usage of the ACPI command when Secure Boot is enabled. This flaw allows an attacker with privileged access to craft a Secondary System Description Table (SSDT) containing code to overwrite the Linux kernel lockdown variable content directly into memory. The table is further loaded and executed by the kernel, defeating its Secure Boot lockdown and allowing the attacker to load unsigned code. The highest threat from this vulnerability is to data confidentiality and integrity, as well as system availability.
CVE-2020-14372	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	A flaw was found in grub2 in versions prior to 2.06, where it incorrectly enables the usage of the ACPI command when Secure Boot is enabled. This flaw allows an attacker with privileged access to craft a Secondary System Description Table (SSDT) containing code to overwrite the Linux kernel lockdown variable content directly into memory. The table is further loaded and executed by the kernel, defeating its Secure Boot lockdown and allowing the attacker to load unsigned code. The highest threat from this vulnerability is to data confidentiality and integrity, as well as system availability.
CVE-2020-14372	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	A flaw was found in grub2 in versions prior to 2.06, where it incorrectly enables the usage of the ACPI command when Secure Boot is enabled. This flaw allows an attacker with privileged access to craft a Secondary System Description Table (SSDT) containing code to overwrite the Linux kernel lockdown variable content directly into memory. The table is further loaded and executed by the kernel, defeating its Secure Boot lockdown and allowing the attacker to load unsigned code. The highest threat from this vulnerability is to data confidentiality and integrity, as well as system availability.
CVE-2020-14372	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	A flaw was found in grub2 in versions prior to 2.06, where it incorrectly enables the usage of the ACPI command when Secure Boot is enabled. This flaw allows an attacker with privileged access to craft a Secondary System Description Table (SSDT) containing code to overwrite the Linux kernel lockdown variable content directly into memory. The table is further loaded and executed by the kernel, defeating its Secure Boot lockdown and allowing the attacker to load unsigned code. The highest threat from this vulnerability is to data confidentiality and integrity, as well as system availability.
CVE-2020-14372	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	A flaw was found in grub2 in versions prior to 2.06, where it incorrectly enables the usage of the ACPI command when Secure Boot is enabled. This flaw allows an attacker with privileged access to craft a Secondary System Description Table (SSDT) containing code to overwrite the Linux kernel lockdown variable content directly into memory. The table is further loaded and executed by the kernel, defeating its Secure Boot lockdown and allowing the attacker to load unsigned code. The highest threat from this vulnerability is to data confidentiality and integrity, as well as system availability.
CVE-2020-14372	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	A flaw was found in grub2 in versions prior to 2.06, where it incorrectly enables the usage of the ACPI command when Secure Boot is enabled. This flaw allows an attacker with privileged access to craft a Secondary System Description Table (SSDT) containing code to overwrite the Linux kernel lockdown variable content directly into memory. The table is further loaded and executed by the kernel, defeating its Secure Boot lockdown and allowing the attacker to load unsigned code. The highest threat from this vulnerability is to data confidentiality and integrity, as well as system availability.
CVE-2020-14372	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	A flaw was found in grub2 in versions prior to 2.06, where it incorrectly enables the usage of the ACPI command when Secure Boot is enabled. This flaw allows an attacker with privileged access to craft a Secondary System Description Table (SSDT) containing code to overwrite the Linux kernel lockdown variable content directly into memory. The table is further loaded and executed by the kernel, defeating its Secure Boot lockdown and allowing the attacker to load unsigned code. The highest threat from this vulnerability is to data confidentiality and integrity, as well as system availability.
CVE-2021-20225	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20225	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20225	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20225	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20225	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20225	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20225	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25647	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	A flaw was found in grub2 in versions prior to 2.06. During USB device initialization, descriptors are read with very little bounds checking and assumes the USB device is providing sane values. If properly exploited, an attacker could trigger memory corruption leading to arbitrary code execution allowing a bypass of the Secure Boot mechanism. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25647	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	A flaw was found in grub2 in versions prior to 2.06. During USB device initialization, descriptors are read with very little bounds checking and assumes the USB device is providing sane values. If properly exploited, an attacker could trigger memory corruption leading to arbitrary code execution allowing a bypass of the Secure Boot mechanism. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25647	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	A flaw was found in grub2 in versions prior to 2.06. During USB device initialization, descriptors are read with very little bounds checking and assumes the USB device is providing sane values. If properly exploited, an attacker could trigger memory corruption leading to arbitrary code execution allowing a bypass of the Secure Boot mechanism. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-25647	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	A flaw was found in grub2 in versions prior to 2.06. During USB device initialization, descriptors are read with very little bounds checking and assumes the USB device is providing sane values. If properly exploited, an attacker could trigger memory corruption leading to arbitrary code execution allowing a bypass of the Secure Boot mechanism. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25647	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	A flaw was found in grub2 in versions prior to 2.06. During USB device initialization, descriptors are read with very little bounds checking and assumes the USB device is providing sane values. If properly exploited, an attacker could trigger memory corruption leading to arbitrary code execution allowing a bypass of the Secure Boot mechanism. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25647	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	A flaw was found in grub2 in versions prior to 2.06. During USB device initialization, descriptors are read with very little bounds checking and assumes the USB device is providing sane values. If properly exploited, an attacker could trigger memory corruption leading to arbitrary code execution allowing a bypass of the Secure Boot mechanism. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25647	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	A flaw was found in grub2 in versions prior to 2.06. During USB device initialization, descriptors are read with very little bounds checking and assumes the USB device is providing sane values. If properly exploited, an attacker could trigger memory corruption leading to arbitrary code execution allowing a bypass of the Secure Boot mechanism. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14308	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process.
CVE-2020-14308	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process.
CVE-2020-14308	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process.
CVE-2020-14308	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process.
CVE-2020-14308	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process.
CVE-2020-14308	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process.
CVE-2020-14308	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process.
CVE-2020-27779	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an privileged attacker to remove address ranges from memory creating an opportunity to circumvent SecureBoot protections after proper triage about grub's memory layout. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27779	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an privileged attacker to remove address ranges from memory creating an opportunity to circumvent SecureBoot protections after proper triage about grub's memory layout. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27779	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an privileged attacker to remove address ranges from memory creating an opportunity to circumvent SecureBoot protections after proper triage about grub's memory layout. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27779	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an privileged attacker to remove address ranges from memory creating an opportunity to circumvent SecureBoot protections after proper triage about grub's memory layout. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27779	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an privileged attacker to remove address ranges from memory creating an opportunity to circumvent SecureBoot protections after proper triage about grub's memory layout. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-27779	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an privileged attacker to remove address ranges from memory creating an opportunity to circumvent SecureBoot protections after proper triage about grub's memory layout. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27779	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an privileged attacker to remove address ranges from memory creating an opportunity to circumvent SecureBoot protections after proper triage about grub's memory layout. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14311	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow.
CVE-2020-14311	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow.
CVE-2020-14311	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow.
CVE-2020-14311	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow.
CVE-2020-14311	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow.
CVE-2020-14311	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow.
CVE-2020-14311	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow.
CVE-2020-27749	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	A flaw was found in grub2 in versions prior to 2.06. Variable names present are expanded in the supplied command line into their corresponding variable contents, using a 1kB stack buffer for temporary storage, without sufficient bounds checking. If the function is called with a command line that references a variable with a sufficiently large payload, it is possible to overflow the stack buffer, corrupt the stack frame and control execution which could also circumvent Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27749	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	A flaw was found in grub2 in versions prior to 2.06. Variable names present are expanded in the supplied command line into their corresponding variable contents, using a 1kB stack buffer for temporary storage, without sufficient bounds checking. If the function is called with a command line that references a variable with a sufficiently large payload, it is possible to overflow the stack buffer, corrupt the stack frame and control execution which could also circumvent Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27749	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	A flaw was found in grub2 in versions prior to 2.06. Variable names present are expanded in the supplied command line into their corresponding variable contents, using a 1kB stack buffer for temporary storage, without sufficient bounds checking. If the function is called with a command line that references a variable with a sufficiently large payload, it is possible to overflow the stack buffer, corrupt the stack frame and control execution which could also circumvent Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27749	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	A flaw was found in grub2 in versions prior to 2.06. Variable names present are expanded in the supplied command line into their corresponding variable contents, using a 1kB stack buffer for temporary storage, without sufficient bounds checking. If the function is called with a command line that references a variable with a sufficiently large payload, it is possible to overflow the stack buffer, corrupt the stack frame and control execution which could also circumvent Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27749	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	A flaw was found in grub2 in versions prior to 2.06. Variable names present are expanded in the supplied command line into their corresponding variable contents, using a 1kB stack buffer for temporary storage, without sufficient bounds checking. If the function is called with a command line that references a variable with a sufficiently large payload, it is possible to overflow the stack buffer, corrupt the stack frame and control execution which could also circumvent Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27749	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	A flaw was found in grub2 in versions prior to 2.06. Variable names present are expanded in the supplied command line into their corresponding variable contents, using a 1kB stack buffer for temporary storage, without sufficient bounds checking. If the function is called with a command line that references a variable with a sufficiently large payload, it is possible to overflow the stack buffer, corrupt the stack frame and control execution which could also circumvent Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27749	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	A flaw was found in grub2 in versions prior to 2.06. Variable names present are expanded in the supplied command line into their corresponding variable contents, using a 1kB stack buffer for temporary storage, without sufficient bounds checking. If the function is called with a command line that references a variable with a sufficiently large payload, it is possible to overflow the stack buffer, corrupt the stack frame and control execution which could also circumvent Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-10713	grub2-2.02-0.87.el7.centos.6.x86_64	grub2	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-10713	grub2-common-2.02-0.87.el7.centos.6.noarch	grub2-common	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-10713	grub2-pc-2.02-0.87.el7.centos.6.x86_64	grub2-pc	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-10713	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch	grub2-pc-modules	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-10713	grub2-tools-2.02-0.87.el7.centos.6.x86_64	grub2-tools	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-10713	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64	grub2-tools-extra	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-10713	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64	grub2-tools-minimal	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2019-19956	libxml2-2.9.1-6.el7.5.x86_64	libxml2	xmlParseBalancedChunkMemoryRecover in parser.c in libxml2 before 2.9.10 has a memory leak related to newDoc->oldNs.
CVE-2019-19956	libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python	xmlParseBalancedChunkMemoryRecover in parser.c in libxml2 before 2.9.10 has a memory leak related to newDoc->oldNs.
CVE-2019-20388	libxml2-2.9.1-6.el7.5.x86_64	libxml2	xmlSchemaPreRun in xmlschemas.c in libxml2 2.9.10 allows an xmlSchemaValidateStream memory leak.
CVE-2019-20388	libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python	xmlSchemaPreRun in xmlschemas.c in libxml2 2.9.10 allows an xmlSchemaValidateStream memory leak.
CVE-2018-14404	libxml2-2.9.1-6.el7.5.x86_64	libxml2	A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 through 2.9.8 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case. Applications processing untrusted XSL format inputs with the use of the libxml2 library may be vulnerable to a denial of service attack due to a crash of the application.
CVE-2018-14404	libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python	A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 through 2.9.8 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case. Applications processing untrusted XSL format inputs with the use of the libxml2 library may be vulnerable to a denial of service attack due to a crash of the application.
CVE-2017-18258	libxml2-2.9.1-6.el7.5.x86_64	libxml2	The xz_head function in xzlib.c in libxml2 before 2.9.6 allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file, because the decoder functionality does not restrict memory usage to what is required for a legitimate file.
CVE-2017-18258	libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python	The xz_head function in xzlib.c in libxml2 before 2.9.6 allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file, because the decoder functionality does not restrict memory usage to what is required for a legitimate file.
CVE-2017-15412	libxml2-2.9.1-6.el7.5.x86_64	libxml2	Use after free in libxml2 before 2.9.5, as used in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15412	libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python	Use after free in libxml2 before 2.9.5, as used in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5131	libxml2-2.9.1-6.el7.5.x86_64	libxml2	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the XPointer range-to function.
CVE-2016-5131	libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the XPointer range-to function.

CVE-2015-8035	libxml2-2.9.1-6.el7.5.x86_64	libxml2	The xz_decomp function in xzlib.c in libxml2 2.9.1 does not properly detect compression errors, which allows context-dependent attackers to cause a denial of service (process hang) via crafted XML data.
CVE-2015-8035	libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python	The xz_decomp function in xzlib.c in libxml2 2.9.1 does not properly detect compression errors, which allows context-dependent attackers to cause a denial of service (process hang) via crafted XML data.
CVE-2020-7595	libxml2-2.9.1-6.el7.5.x86_64	libxml2	xmlStringLenDecodeEntities in parser.c in libxml2 2.9.10 has an infinite loop in a certain end-of-file situation.
CVE-2020-7595	libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python	xmlStringLenDecodeEntities in parser.c in libxml2 2.9.10 has an infinite loop in a certain end-of-file situation.
CVE-2018-1456	libxml2-2.9.1-6.el7.5.x86_64	libxml2	IBM Rhapsody DM 5.0 through 5.0.2 and 6.0 through 6.0.5 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 140091.
CVE-2018-1456	libxml2-python-2.9.1-6.el7.5.x86_64	libxml2-python	IBM Rhapsody DM 5.0 through 5.0.2 and 6.0 through 6.0.5 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 140091.
CVE-2021-27364	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.
CVE-2021-27364	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.
CVE-2021-27364	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.
CVE-2021-27364	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.
CVE-2021-27364	perf-3.10.0-1160.31.1.el7.x86_64	perf	An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.
CVE-2020-25643	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read overflow is caused by improper input validation in the ppp_cp_parse_cr function which can cause the system to crash or cause a denial of service. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25643	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read overflow is caused by improper input validation in the ppp_cp_parse_cr function which can cause the system to crash or cause a denial of service. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25643	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read overflow is caused by improper input validation in the ppp_cp_parse_cr function which can cause the system to crash or cause a denial of service. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25643	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read overflow is caused by improper input validation in the ppp_cp_parse_cr function which can cause the system to crash or cause a denial of service. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25643	perf-3.10.0-1160.31.1.el7.x86_64	perf	A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read overflow is caused by improper input validation in the ppp_cp_parse_cr function which can cause the system to crash or cause a denial of service. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25705	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A flaw in the way reply ICMP packets are limited in the Linux kernel functionality was found that allows to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypassing source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.
CVE-2020-25705	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A flaw in the way reply ICMP packets are limited in the Linux kernel functionality was found that allows to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypassing source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.
CVE-2020-25705	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A flaw in the way reply ICMP packets are limited in the Linux kernel functionality was found that allows to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypassing source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.

CVE-2020-25705	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A flaw in the way reply ICMP packets are limited in the Linux kernel functionality was found that allows to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypassing source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.
CVE-2020-25705	perf-3.10.0-1160.31.1.el7.x86_64	perf	A flaw in the way reply ICMP packets are limited in the Linux kernel functionality was found that allows to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypassing source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.
CVE-2021-27365	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.
CVE-2021-27365	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.
CVE-2021-27365	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.
CVE-2021-27365	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.
CVE-2021-27365	perf-3.10.0-1160.31.1.el7.x86_64	perf	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.
CVE-2021-3347	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.
CVE-2021-3347	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.
CVE-2021-3347	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.
CVE-2021-3347	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.
CVE-2021-3347	perf-3.10.0-1160.31.1.el7.x86_64	perf	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.
CVE-2020-28374	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.
CVE-2020-28374	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.
CVE-2020-28374	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.
CVE-2020-28374	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.
CVE-2020-28374	perf-3.10.0-1160.31.1.el7.x86_64	perf	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.
CVE-2020-29661	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.

CVE-2020-29661	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.
CVE-2020-29661	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.
CVE-2020-29661	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.
CVE-2020-29661	perf-3.10.0-1160.31.1.el7.x86_64	perf	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.
CVE-2020-14314	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A memory out-of-bounds read flaw was found in the Linux kernel before 5.9-rc2 with the ext3/ext4 file system, in the way it accesses a directory with broken indexing. This flaw allows a local user to crash the system if the directory exists. The highest threat from this vulnerability is to system availability.
CVE-2020-14314	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A memory out-of-bounds read flaw was found in the Linux kernel before 5.9-rc2 with the ext3/ext4 file system, in the way it accesses a directory with broken indexing. This flaw allows a local user to crash the system if the directory exists. The highest threat from this vulnerability is to system availability.
CVE-2020-14314	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A memory out-of-bounds read flaw was found in the Linux kernel before 5.9-rc2 with the ext3/ext4 file system, in the way it accesses a directory with broken indexing. This flaw allows a local user to crash the system if the directory exists. The highest threat from this vulnerability is to system availability.
CVE-2020-14314	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A memory out-of-bounds read flaw was found in the Linux kernel before 5.9-rc2 with the ext3/ext4 file system, in the way it accesses a directory with broken indexing. This flaw allows a local user to crash the system if the directory exists. The highest threat from this vulnerability is to system availability.
CVE-2020-14314	perf-3.10.0-1160.31.1.el7.x86_64	perf	A memory out-of-bounds read flaw was found in the Linux kernel before 5.9-rc2 with the ext3/ext4 file system, in the way it accesses a directory with broken indexing. This flaw allows a local user to crash the system if the directory exists. The highest threat from this vulnerability is to system availability.
CVE-2020-25211	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c, aka CID-1cc5ef91d2ff.
CVE-2020-25211	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c, aka CID-1cc5ef91d2ff.
CVE-2020-25211	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c, aka CID-1cc5ef91d2ff.
CVE-2020-25211	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c, aka CID-1cc5ef91d2ff.
CVE-2020-25211	perf-3.10.0-1160.31.1.el7.x86_64	perf	In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c, aka CID-1cc5ef91d2ff.
CVE-2020-15436	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	Use-after-free vulnerability in fs/block_dev.c in the Linux kernel before 5.8 allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field.
CVE-2020-15436	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	Use-after-free vulnerability in fs/block_dev.c in the Linux kernel before 5.8 allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field.
CVE-2020-15436	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	Use-after-free vulnerability in fs/block_dev.c in the Linux kernel before 5.8 allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field.

CVE-2020-15436	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	Use-after-free vulnerability in fs/block_dev.c in the Linux kernel before 5.8 allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field.
CVE-2020-15436	perf-3.10.0-1160.31.1.el7.x86_64	perf	Use-after-free vulnerability in fs/block_dev.c in the Linux kernel before 5.8 allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field.
CVE-2020-25645	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.
CVE-2020-25645	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.
CVE-2020-25645	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.
CVE-2020-25645	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.
CVE-2020-25645	perf-3.10.0-1160.31.1.el7.x86_64	perf	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.
CVE-2020-14351	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14351	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14351	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14351	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14351	perf-3.10.0-1160.31.1.el7.x86_64	perf	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-12362	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	Integer overflow in the firmware for some Intel(R) Graphics Drivers for Windows * before version 26.20.100.7212 and before Linux kernel version 5.5 may allow a privileged user to potentially enable an escalation of privilege via local access.
CVE-2020-12362	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	Integer overflow in the firmware for some Intel(R) Graphics Drivers for Windows * before version 26.20.100.7212 and before Linux kernel version 5.5 may allow a privileged user to potentially enable an escalation of privilege via local access.
CVE-2020-12362	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	Integer overflow in the firmware for some Intel(R) Graphics Drivers for Windows * before version 26.20.100.7212 and before Linux kernel version 5.5 may allow a privileged user to potentially enable an escalation of privilege via local access.
CVE-2020-12362	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	Integer overflow in the firmware for some Intel(R) Graphics Drivers for Windows * before version 26.20.100.7212 and before Linux kernel version 5.5 may allow a privileged user to potentially enable an escalation of privilege via local access.
CVE-2020-12362	perf-3.10.0-1160.31.1.el7.x86_64	perf	Integer overflow in the firmware for some Intel(R) Graphics Drivers for Windows * before version 26.20.100.7212 and before Linux kernel version 5.5 may allow a privileged user to potentially enable an escalation of privilege via local access.
CVE-2020-7053	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	In the Linux kernel 4.14 longterm through 4.14.165 and 4.19 longterm through 4.19.96 (and 5.x before 5.2), there is a use-after-free (write) in the i915_ppgtt_close function in drivers /gpu/drm/i915/i915_gem_gtt.c, aka CID-7dc40713618c. This is related to i915_gem_context_destroy_ioctl in drivers/gpu/drm/i915/i915_gem_context.c.

CVE-2020-7053	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	In the Linux kernel 4.14 longterm through 4.14.165 and 4.19 longterm through 4.19.96 (and 5.x before 5.2), there is a use-after-free (write) in the i915_ppgtt_close function in drivers/gpu/drm/i915/i915_gem_gtt.c, aka CID-7dc40713618c. This is related to i915_gem_context_destroy_ioctl in drivers/gpu/drm/i915/i915_gem_context.c.
CVE-2020-7053	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	In the Linux kernel 4.14 longterm through 4.14.165 and 4.19 longterm through 4.19.96 (and 5.x before 5.2), there is a use-after-free (write) in the i915_ppgtt_close function in drivers/gpu/drm/i915/i915_gem_gtt.c, aka CID-7dc40713618c. This is related to i915_gem_context_destroy_ioctl in drivers/gpu/drm/i915/i915_gem_context.c.
CVE-2020-7053	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	In the Linux kernel 4.14 longterm through 4.14.165 and 4.19 longterm through 4.19.96 (and 5.x before 5.2), there is a use-after-free (write) in the i915_ppgtt_close function in drivers/gpu/drm/i915/i915_gem_gtt.c, aka CID-7dc40713618c. This is related to i915_gem_context_destroy_ioctl in drivers/gpu/drm/i915/i915_gem_context.c.
CVE-2020-7053	perf-3.10.0-1160.31.1.el7.x86_64	perf	In the Linux kernel 4.14 longterm through 4.14.165 and 4.19 longterm through 4.19.96 (and 5.x before 5.2), there is a use-after-free (write) in the i915_ppgtt_close function in drivers/gpu/drm/i915/i915_gem_gtt.c, aka CID-7dc40713618c. This is related to i915_gem_context_destroy_ioctl in drivers/gpu/drm/i915/i915_gem_context.c.
CVE-2020-8648	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.
CVE-2020-8648	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.
CVE-2020-8648	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.
CVE-2020-8648	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.
CVE-2020-8648	perf-3.10.0-1160.31.1.el7.x86_64	perf	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.
CVE-2020-10769	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A buffer over-read flaw was found in RH kernel versions before 5.0 in crypto_authenc_extractkeys in crypto/authenc.c in the IPsec Cryptographic algorithm's module, authenc. When a payload longer than 4 bytes, and is not following 4-byte alignment boundary guidelines, it causes a buffer over-read threat, leading to a system crash. This flaw allows a local attacker with user privileges to cause a denial of service.
CVE-2020-10769	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A buffer over-read flaw was found in RH kernel versions before 5.0 in crypto_authenc_extractkeys in crypto/authenc.c in the IPsec Cryptographic algorithm's module, authenc. When a payload longer than 4 bytes, and is not following 4-byte alignment boundary guidelines, it causes a buffer over-read threat, leading to a system crash. This flaw allows a local attacker with user privileges to cause a denial of service.
CVE-2020-10769	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A buffer over-read flaw was found in RH kernel versions before 5.0 in crypto_authenc_extractkeys in crypto/authenc.c in the IPsec Cryptographic algorithm's module, authenc. When a payload longer than 4 bytes, and is not following 4-byte alignment boundary guidelines, it causes a buffer over-read threat, leading to a system crash. This flaw allows a local attacker with user privileges to cause a denial of service.
CVE-2020-10769	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A buffer over-read flaw was found in RH kernel versions before 5.0 in crypto_authenc_extractkeys in crypto/authenc.c in the IPsec Cryptographic algorithm's module, authenc. When a payload longer than 4 bytes, and is not following 4-byte alignment boundary guidelines, it causes a buffer over-read threat, leading to a system crash. This flaw allows a local attacker with user privileges to cause a denial of service.
CVE-2020-10769	perf-3.10.0-1160.31.1.el7.x86_64	perf	A buffer over-read flaw was found in RH kernel versions before 5.0 in crypto_authenc_extractkeys in crypto/authenc.c in the IPsec Cryptographic algorithm's module, authenc. When a payload longer than 4 bytes, and is not following 4-byte alignment boundary guidelines, it causes a buffer over-read threat, leading to a system crash. This flaw allows a local attacker with user privileges to cause a denial of service.
CVE-2019-18282	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	The flow_dissector feature in the Linux kernel 4.3 through 5.x before 5.3.10 has a device tracking vulnerability, aka CID-55667441c84f. This occurs because the auto flowlabel of a UDP IPv6 packet relies on a 32-bit hashrnd value as a secret, and because jhash (instead of siphash) is used. The hashrnd value remains the same starting from boot time, and can be inferred by an attacker. This affects net/core/flow_dissector.c and related code.
CVE-2019-18282	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	The flow_dissector feature in the Linux kernel 4.3 through 5.x before 5.3.10 has a device tracking vulnerability, aka CID-55667441c84f. This occurs because the auto flowlabel of a UDP IPv6 packet relies on a 32-bit hashrnd value as a secret, and because jhash (instead of siphash) is used. The hashrnd value remains the same starting from boot time, and can be inferred by an attacker. This affects net/core/flow_dissector.c and related code.
CVE-2019-18282	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	The flow_dissector feature in the Linux kernel 4.3 through 5.x before 5.3.10 has a device tracking vulnerability, aka CID-55667441c84f. This occurs because the auto flowlabel of a UDP IPv6 packet relies on a 32-bit hashrnd value as a secret, and because jhash (instead of siphash) is used. The hashrnd value remains the same starting from boot time, and can be inferred by an attacker. This affects net/core/flow_dissector.c and related code.

CVE-2019-18282	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	The flow_dissector feature in the Linux kernel 4.3 through 5.x before 5.3.10 has a device tracking vulnerability, aka CID-55667441c84f. This occurs because the auto flowlabel of a UDP IPv6 packet relies on a 32-bit hashrnd value as a secret, and because jhash (instead of siphash) is used. The hashrnd value remains the same starting from boot time, and can be inferred by an attacker. This affects net/core/flow_dissector.c and related code.
CVE-2019-18282	perf-3.10.0-1160.31.1.el7.x86_64	perf	The flow_dissector feature in the Linux kernel 4.3 through 5.x before 5.3.10 has a device tracking vulnerability, aka CID-55667441c84f. This occurs because the auto flowlabel of a UDP IPv6 packet relies on a 32-bit hashrnd value as a secret, and because jhash (instead of siphash) is used. The hashrnd value remains the same starting from boot time, and can be inferred by an attacker. This affects net/core/flow_dissector.c and related code.
CVE-2020-25656	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality.
CVE-2020-25656	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality.
CVE-2020-25656	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality.
CVE-2020-25656	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality.
CVE-2020-25656	perf-3.10.0-1160.31.1.el7.x86_64	perf	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality.
CVE-2019-19532	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	In the Linux kernel before 5.3.9, there are multiple out-of-bounds write bugs that can be caused by a malicious USB device in the Linux kernel HID drivers, aka CID-d9d4b1e46d95. This affects drivers/hid/hid-axff.c, drivers/hid/hid-dr.c, drivers/hid/hid-emsff.c, drivers/hid/hid-gaff.c, drivers/hid/hid-holtekff.c, drivers/hid/hid-lg2ff.c, drivers/hid/hid-lg3ff.c, drivers/hid/hid-lg4ff.c, drivers/hid/hid-lgff.c, drivers/hid/hid-logitech-hidpp.c, drivers/hid/hid-microsoft.c, drivers/hid/hid-sony.c, drivers/hid/hid-tmff.c, and drivers/hid/hid-zpff.c.
CVE-2019-19532	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	In the Linux kernel before 5.3.9, there are multiple out-of-bounds write bugs that can be caused by a malicious USB device in the Linux kernel HID drivers, aka CID-d9d4b1e46d95. This affects drivers/hid/hid-axff.c, drivers/hid/hid-dr.c, drivers/hid/hid-emsff.c, drivers/hid/hid-gaff.c, drivers/hid/hid-holtekff.c, drivers/hid/hid-lg2ff.c, drivers/hid/hid-lg3ff.c, drivers/hid/hid-lg4ff.c, drivers/hid/hid-lgff.c, drivers/hid/hid-logitech-hidpp.c, drivers/hid/hid-microsoft.c, drivers/hid/hid-sony.c, drivers/hid/hid-tmff.c, and drivers/hid/hid-zpff.c.
CVE-2019-19532	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	In the Linux kernel before 5.3.9, there are multiple out-of-bounds write bugs that can be caused by a malicious USB device in the Linux kernel HID drivers, aka CID-d9d4b1e46d95. This affects drivers/hid/hid-axff.c, drivers/hid/hid-dr.c, drivers/hid/hid-emsff.c, drivers/hid/hid-gaff.c, drivers/hid/hid-holtekff.c, drivers/hid/hid-lg2ff.c, drivers/hid/hid-lg3ff.c, drivers/hid/hid-lg4ff.c, drivers/hid/hid-lgff.c, drivers/hid/hid-logitech-hidpp.c, drivers/hid/hid-microsoft.c, drivers/hid/hid-sony.c, drivers/hid/hid-tmff.c, and drivers/hid/hid-zpff.c.
CVE-2019-19532	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	In the Linux kernel before 5.3.9, there are multiple out-of-bounds write bugs that can be caused by a malicious USB device in the Linux kernel HID drivers, aka CID-d9d4b1e46d95. This affects drivers/hid/hid-axff.c, drivers/hid/hid-dr.c, drivers/hid/hid-emsff.c, drivers/hid/hid-gaff.c, drivers/hid/hid-holtekff.c, drivers/hid/hid-lg2ff.c, drivers/hid/hid-lg3ff.c, drivers/hid/hid-lg4ff.c, drivers/hid/hid-lgff.c, drivers/hid/hid-logitech-hidpp.c, drivers/hid/hid-microsoft.c, drivers/hid/hid-sony.c, drivers/hid/hid-tmff.c, and drivers/hid/hid-zpff.c.
CVE-2019-19532	perf-3.10.0-1160.31.1.el7.x86_64	perf	In the Linux kernel before 5.3.9, there are multiple out-of-bounds write bugs that can be caused by a malicious USB device in the Linux kernel HID drivers, aka CID-d9d4b1e46d95. This affects drivers/hid/hid-axff.c, drivers/hid/hid-dr.c, drivers/hid/hid-emsff.c, drivers/hid/hid-gaff.c, drivers/hid/hid-holtekff.c, drivers/hid/hid-lg2ff.c, drivers/hid/hid-lg3ff.c, drivers/hid/hid-lg4ff.c, drivers/hid/hid-lgff.c, drivers/hid/hid-logitech-hidpp.c, drivers/hid/hid-microsoft.c, drivers/hid/hid-sony.c, drivers/hid/hid-tmff.c, and drivers/hid/hid-zpff.c.
CVE-2020-14385	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A flaw was found in the Linux kernel before 5.9-rc4. A failure of the file system metadata validator in XFS can cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt. This can lead to the filesystem being shutdown, or otherwise rendered inaccessible until it is remounted, leading to a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-14385	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A flaw was found in the Linux kernel before 5.9-rc4. A failure of the file system metadata validator in XFS can cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt. This can lead to the filesystem being shutdown, or otherwise rendered inaccessible until it is remounted, leading to a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-14385	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A flaw was found in the Linux kernel before 5.9-rc4. A failure of the file system metadata validator in XFS can cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt. This can lead to the filesystem being shutdown, or otherwise rendered inaccessible until it is remounted, leading to a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-14385	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A flaw was found in the Linux kernel before 5.9-rc4. A failure of the file system metadata validator in XFS can cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt. This can lead to the filesystem being shutdown, or otherwise rendered inaccessible until it is remounted, leading to a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-14385	perf-3.10.0-1160.31.1.el7.x86_64	perf	A flaw was found in the Linux kernel before 5.9-rc4. A failure of the file system metadata validator in XFS can cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt. This can lead to the filesystem being shutdown, or otherwise rendered inaccessible until it is remounted, leading to a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2021-27363	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the iscsi_transport structure. When an iSCSI transport is registered with the iSCSI subsystem, the transport's handle is available to unprivileged users via the sysfs file system, at /sys/class/iscsi_transport/$TRANSPORT_NAME/handle. When read, the show_transport_handle function (in drivers/scsi/scsi_transport_iscsi.c) is called, which leaks the handle. This handle is actually the pointer to an iscsi_transport struct in the kernel module's global variables.

CVE-2021-27363	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the iscsi_transport structure. When an iSCSI transport is registered with the iSCSI subsystem, the transport's handle is available to unprivileged users via the sysfs file system, at /sys/class/iscsi_transport/$TRANSPORT_NAME/handle. When read, the show_transport_handle function (in drivers/scsi/scsi_transport_iscsi.c) is called, which leaks the handle. This handle is actually the pointer to an iscsi_transport struct in the kernel module's global variables.
CVE-2021-27363	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the iscsi_transport structure. When an iSCSI transport is registered with the iSCSI subsystem, the transport's handle is available to unprivileged users via the sysfs file system, at /sys/class/iscsi_transport/$TRANSPORT_NAME/handle. When read, the show_transport_handle function (in drivers/scsi/scsi_transport_iscsi.c) is called, which leaks the handle. This handle is actually the pointer to an iscsi_transport struct in the kernel module's global variables.
CVE-2021-27363	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the iscsi_transport structure. When an iSCSI transport is registered with the iSCSI subsystem, the transport's handle is available to unprivileged users via the sysfs file system, at /sys/class/iscsi_transport/$TRANSPORT_NAME/handle. When read, the show_transport_handle function (in drivers/scsi/scsi_transport_iscsi.c) is called, which leaks the handle. This handle is actually the pointer to an iscsi_transport struct in the kernel module's global variables.
CVE-2021-27363	perf-3.10.0-1160.31.1.el7.x86_64	perf	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the iscsi_transport structure. When an iSCSI transport is registered with the iSCSI subsystem, the transport's handle is available to unprivileged users via the sysfs file system, at /sys/class/iscsi_transport/$TRANSPORT_NAME/handle. When read, the show_transport_handle function (in drivers/scsi/scsi_transport_iscsi.c) is called, which leaks the handle. This handle is actually the pointer to an iscsi_transport struct in the kernel module's global variables.
CVE-2020-25212	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs/nfs4proc.c instead of fs/nfs/nfs4xdr.c, aka CID-b4487b935452.
CVE-2020-25212	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs/nfs4proc.c instead of fs/nfs/nfs4xdr.c, aka CID-b4487b935452.
CVE-2020-25212	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs/nfs4proc.c instead of fs/nfs/nfs4xdr.c, aka CID-b4487b935452.
CVE-2020-25212	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs/nfs4proc.c instead of fs/nfs/nfs4xdr.c, aka CID-b4487b935452.
CVE-2020-25212	perf-3.10.0-1160.31.1.el7.x86_64	perf	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs/nfs4proc.c instead of fs/nfs/nfs4xdr.c, aka CID-b4487b935452.
CVE-2020-27170	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 5.11.8. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory, aka CID-f232326f6966. This affects pointer types that do not define a ptr_limit.
CVE-2020-27170	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	An issue was discovered in the Linux kernel before 5.11.8. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory, aka CID-f232326f6966. This affects pointer types that do not define a ptr_limit.
CVE-2020-27170	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	An issue was discovered in the Linux kernel before 5.11.8. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory, aka CID-f232326f6966. This affects pointer types that do not define a ptr_limit.
CVE-2020-27170	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	An issue was discovered in the Linux kernel before 5.11.8. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory, aka CID-f232326f6966. This affects pointer types that do not define a ptr_limit.
CVE-2020-27170	perf-3.10.0-1160.31.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 5.11.8. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory, aka CID-f232326f6966. This affects pointer types that do not define a ptr_limit.
CVE-2020-0427	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	In create_pinctrl of core.c, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-140550171
CVE-2020-0427	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	In create_pinctrl of core.c, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-140550171
CVE-2020-0427	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	In create_pinctrl of core.c, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-140550171

CVE-2020-0427	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	In create_pinctrl of core.c, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-140550171
CVE-2020-0427	perf-3.10.0-1160.31.1.el7.x86_64	perf	In create_pinctrl of core.c, there is a possible out of bounds read due to a use after free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-140550171
CVE-2020-24394	kernel-3.10.0-1160.31.1.el7.x86_64	kernel	In the Linux kernel before 5.7.8, fs/nfsd/vfs.c (in the NFS server) can set incorrect permissions on new filesystem objects when the filesystem lacks ACL support, aka CID-22cf8419f131. This occurs because the current umask is not considered.
CVE-2020-24394	kernel-devel-3.10.0-1160.31.1.el7.x86_64	kernel-devel	In the Linux kernel before 5.7.8, fs/nfsd/vfs.c (in the NFS server) can set incorrect permissions on new filesystem objects when the filesystem lacks ACL support, aka CID-22cf8419f131. This occurs because the current umask is not considered.
CVE-2020-24394	kernel-tools-3.10.0-1160.31.1.el7.x86_64	kernel-tools	In the Linux kernel before 5.7.8, fs/nfsd/vfs.c (in the NFS server) can set incorrect permissions on new filesystem objects when the filesystem lacks ACL support, aka CID-22cf8419f131. This occurs because the current umask is not considered.
CVE-2020-24394	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64	kernel-tools-libs	In the Linux kernel before 5.7.8, fs/nfsd/vfs.c (in the NFS server) can set incorrect permissions on new filesystem objects when the filesystem lacks ACL support, aka CID-22cf8419f131. This occurs because the current umask is not considered.
CVE-2020-24394	perf-3.10.0-1160.31.1.el7.x86_64	perf	In the Linux kernel before 5.7.8, fs/nfsd/vfs.c (in the NFS server) can set incorrect permissions on new filesystem objects when the filesystem lacks ACL support, aka CID-22cf8419f131. This occurs because the current umask is not considered.
CVE-2020-11868	ntp-4.2.6p5-29.el7.centos.2.x86_64	ntp	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp.
CVE-2020-11868	ntpdate-4.2.6p5-29.el7.centos.2.x86_64	ntpdate	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp.
CVE-2020-12243	openldap-2.4.44-23.el7_9.x86_64	openldap	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).
CVE-2020-25692	openldap-2.4.44-23.el7_9.x86_64	openldap	A NULL pointer dereference was found in OpenLDAP server and was fixed in openldap 2.4.55, during a request for renaming RDNs. An unauthenticated attacker could remotely crash the slapd process by sending a specially crafted request, causing a Denial of Service.
CVE-2020-14363	libX11-1.6.7-3.el7_9.x86_64	libX11	An integer overflow vulnerability leading to a double-free was found in libX11. This flaw allows a local privileged attacker to cause an application compiled with libX11 to crash, or in some cases, result in arbitrary code execution. The highest threat from this flaw is to confidentiality, integrity as well as system availability.
CVE-2020-14363	libX11-common-1.6.7-3.el7_9.noarch	libX11-common	An integer overflow vulnerability leading to a double-free was found in libX11. This flaw allows a local privileged attacker to cause an application compiled with libX11 to crash, or in some cases, result in arbitrary code execution. The highest threat from this flaw is to confidentiality, integrity as well as system availability.
CVE-2020-12825	libcroco-0.6.12-6.el7_9.x86_64	libcroco	libcroco through 0.6.13 has excessive recursion in cr_parser_parse_any_core in cr-parser.c, leading to stack consumption.
CVE-2021-20277	libldb-1.5.4-2.el7.x86_64	libldb	A flaw was found in Samba's libldb. Multiple, consecutive leading spaces in an LDAP attribute can lead to an out-of-bounds memory write, leading to a crash of the LDAP server process handling the request. The highest threat from this vulnerability is to system availability.
CVE-2019-1010305	libmspack-0.5-0.8.alpha.el7.x86_64	libmspack	libmspack 0.9.1alpha is affected by: Buffer Overflow. The impact is: Information Disclosure. The component is: function chmd_read_headers() in libmspack(file libmspack/mspack/chmd.c). The attack vector is: the victim must open a specially crafted chm file. The fixed version is: after commit 2f084136cfe0d05e5bf5703f3e83c6d955234b4d.
CVE-2019-17498	libssh2-1.8.0-4.el7.x86_64	libssh2	In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, enabling an attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server.
CVE-2020-14318	libwbclient-4.10.16-15.el7_9.x86_64	libwbclient	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14318	samba-4.10.16-15.el7_9.x86_64	samba	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14318	samba-client-libs-4.10.16-15.el7_9.x86_64	samba-client-libs	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14318	samba-common-4.10.16-15.el7_9.noarch	samba-common	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.

CVE-2020-14318	samba-common-libs-4.10.16-15.el7_9.x86_64	samba-common-libs	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14318	samba-common-tools-4.10.16-15.el7_9.x86_64	samba-common-tools	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14318	samba-libs-4.10.16-15.el7_9.x86_64	samba-libs	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14318	samba-winbind-4.10.16-15.el7_9.x86_64	samba-winbind	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14318	samba-winbind-clients-4.10.16-15.el7_9.x86_64	samba-winbind-clients	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14318	samba-winbind-modules-4.10.16-15.el7_9.x86_64	samba-winbind-modules	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2021-20254	libwbclient-4.10.16-15.el7_9.x86_64	libwbclient	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20254	samba-4.10.16-15.el7_9.x86_64	samba	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20254	samba-client-libs-4.10.16-15.el7_9.x86_64	samba-client-libs	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20254	samba-common-4.10.16-15.el7_9.noarch	samba-common	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20254	samba-common-libs-4.10.16-15.el7_9.x86_64	samba-common-libs	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20254	samba-common-tools-4.10.16-15.el7_9.x86_64	samba-common-tools	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20254	samba-libs-4.10.16-15.el7_9.x86_64	samba-libs	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20254	samba-winbind-4.10.16-15.el7_9.x86_64	samba-winbind	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20254	samba-winbind-clients-4.10.16-15.el7_9.x86_64	samba-winbind-clients	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20254	samba-winbind-modules-4.10.16-15.el7_9.x86_64	samba-winbind-modules	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2019-10197	libwbclient-4.10.16-15.el7_9.x86_64	libwbclient	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10197	samba-4.10.16-15.el7_9.x86_64	samba	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10197	samba-client-libs-4.10.16-15.el7_9.x86_64	samba-client-libs	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.

CVE-2019-10197	samba-common-4.10.16-15.el7_9.noarch	samba-common	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10197	samba-common-libs-4.10.16-15.el7_9.x86_64	samba-common-libs	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10197	samba-common-tools-4.10.16-15.el7_9.x86_64	samba-common-tools	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10197	samba-libs-4.10.16-15.el7_9.x86_64	samba-libs	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10197	samba-winbind-4.10.16-15.el7_9.x86_64	samba-winbind	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10197	samba-winbind-clients-4.10.16-15.el7_9.x86_64	samba-winbind-clients	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10197	samba-winbind-modules-4.10.16-15.el7_9.x86_64	samba-winbind-modules	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10218	libwbclient-4.10.16-15.el7_9.x86_64	libwbclient	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10218	samba-4.10.16-15.el7_9.x86_64	samba	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10218	samba-client-libs-4.10.16-15.el7_9.x86_64	samba-client-libs	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10218	samba-common-4.10.16-15.el7_9.noarch	samba-common	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10218	samba-common-libs-4.10.16-15.el7_9.x86_64	samba-common-libs	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10218	samba-common-tools-4.10.16-15.el7_9.x86_64	samba-common-tools	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10218	samba-libs-4.10.16-15.el7_9.x86_64	samba-libs	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10218	samba-winbind-4.10.16-15.el7_9.x86_64	samba-winbind	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10218	samba-winbind-clients-4.10.16-15.el7_9.x86_64	samba-winbind-clients	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10218	samba-winbind-modules-4.10.16-15.el7_9.x86_64	samba-winbind-modules	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2020-1472	libwbclient-4.10.16-15.el7_9.x86_64	libwbclient	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-1472	samba-4.10.16-15.el7_9.x86_64	samba	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.

CVE-2020-1472	samba-client-libs-4.10.16-15.el7_9.x86_64	samba-client-libs	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-1472	samba-common-4.10.16-15.el7_9.noarch	samba-common	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-1472	samba-common-libs-4.10.16-15.el7_9.x86_64	samba-common-libs	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-1472	samba-common-tools-4.10.16-15.el7_9.x86_64	samba-common-tools	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-1472	samba-libs-4.10.16-15.el7_9.x86_64	samba-libs	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-1472	samba-winbind-4.10.16-15.el7_9.x86_64	samba-winbind	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-1472	samba-winbind-clients-4.10.16-15.el7_9.x86_64	samba-winbind-clients	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-1472	samba-winbind-modules-4.10.16-15.el7_9.x86_64	samba-winbind-modules	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-14323	libwbclient-4.10.16-15.el7_9.x86_64	libwbclient	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14323	samba-4.10.16-15.el7_9.x86_64	samba	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14323	samba-client-libs-4.10.16-15.el7_9.x86_64	samba-client-libs	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14323	samba-common-4.10.16-15.el7_9.noarch	samba-common	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14323	samba-common-libs-4.10.16-15.el7_9.x86_64	samba-common-libs	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14323	samba-common-tools-4.10.16-15.el7_9.x86_64	samba-common-tools	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14323	samba-libs-4.10.16-15.el7_9.x86_64	samba-libs	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14323	samba-winbind-4.10.16-15.el7_9.x86_64	samba-winbind	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14323	samba-winbind-clients-4.10.16-15.el7_9.x86_64	samba-winbind-clients	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14323	samba-winbind-modules-4.10.16-15.el7_9.x86_64	samba-winbind-modules	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2019-14907	libwbclient-4.10.16-15.el7_9.x86_64	libwbclient	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).

CVE-2019-14907	samba-4.10.16-15.el7_9.x86_64	samba	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2019-14907	samba-client-libs-4.10.16-15.el7_9.x86_64	samba-client-libs	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2019-14907	samba-common-4.10.16-15.el7_9.noarch	samba-common	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2019-14907	samba-common-libs-4.10.16-15.el7_9.x86_64	samba-common-libs	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2019-14907	samba-common-tools-4.10.16-15.el7_9.x86_64	samba-common-tools	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2019-14907	samba-libs-4.10.16-15.el7_9.x86_64	samba-libs	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2019-14907	samba-winbind-4.10.16-15.el7_9.x86_64	samba-winbind	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2019-14907	samba-winbind-clients-4.10.16-15.el7_9.x86_64	samba-winbind-clients	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2019-14907	samba-winbind-modules-4.10.16-15.el7_9.x86_64	samba-winbind-modules	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2020-0549	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Cleanup errors in some data cache evictions for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-0548	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Cleanup errors in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2019-11135	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	TSX Asynchronous Abort condition on some CPUs utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
CVE-2017-5715	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Systems with microprocessors utilizing speculative execution andindirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2019-11139	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Improper conditions check in the voltage modulation interface for some Intel(R) Xeon(R) Scalable Processors may allow a privileged user to potentially enable denial of service via local access.
CVE-2020-8695	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Observable discrepancy in the RAPL interface for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.
CVE-2020-8698	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Improper isolation of shared resources in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-8694	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Insufficient access control in the Linux kernel driver for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2019-0117	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Insufficient access control in protected memory subsystem for Intel(R) SGX for 6th, 7th, 8th, 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Xeon(R) Processor E3-1500 v5, v6 Families; Intel(R) Xeon(R) E-2100 & E-2200 Processor Families with Intel(R) Processor Graphics may allow a privileged user to potentially enable information disclosure via local access.
CVE-2020-8696	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Improper removal of sensitive information before storage or transfer in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVE-2020-0543	microcode_ctl-2.1-73.8.el7_9.x86_64	microcode_ctl	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-15862	net-snmp-5.7.2-49.el7_9.1.x86_64	net-snmp	Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.
CVE-2020-15862	net-snmp-agent-libs-5.7.2-49.el7_9.1.x86_64	net-snmp-agent-libs	Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.
CVE-2020-15862	net-snmp-libs-5.7.2-49.el7_9.1.x86_64	net-snmp-libs	Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.
CVE-2020-15862	net-snmp-perl-5.7.2-49.el7_9.1.x86_64	net-snmp-perl	Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.
CVE-2020-15862	net-snmp-utils-5.7.2-49.el7_9.1.x86_64	net-snmp-utils	Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.
CVE-2018-18066	net-snmp-5.7.2-49.el7_9.1.x86_64	net-snmp	snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2018-18066	net-snmp-agent-libs-5.7.2-49.el7_9.1.x86_64	net-snmp-agent-libs	snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2018-18066	net-snmp-libs-5.7.2-49.el7_9.1.x86_64	net-snmp-libs	snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2018-18066	net-snmp-perl-5.7.2-49.el7_9.1.x86_64	net-snmp-perl	snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2018-18066	net-snmp-utils-5.7.2-49.el7_9.1.x86_64	net-snmp-utils	snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2019-2737	mariadb-libs-5.5.68-1.el7.x86_64	mariadb-libs	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2805	mariadb-libs-5.5.68-1.el7.x86_64	mariadb-libs	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2739	mariadb-libs-5.5.68-1.el7.x86_64	mariadb-libs	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2020-2574	mariadb-libs-5.5.68-1.el7.x86_64	mariadb-libs	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.46 and prior, 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2740	mariadb-libs-5.5.68-1.el7.x86_64	mariadb-libs	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2780	mariadb-libs-5.5.68-1.el7.x86_64	mariadb-libs	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2974	mariadb-libs-5.5.68-1.el7.x86_64	mariadb-libs	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.45 and prior, 5.7.27 and prior and 8.0.17 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
cve-2020-1971	openssl-1.0.2k-21.el7_9.x86_64	openssl	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

cve-2020-1971	openssl-libs-1.0.2k-21.el7_9.x86_64	openssl-libs	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).
CVE-2020-1971	openssl-1.0.2k-21.el7_9.x86_64	openssl	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).
CVE-2020-1971	openssl-libs-1.0.2k-21.el7_9.x86_64	openssl-libs	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).
CVE-2018-1116	polkit-0.112-26.el7.x86_64	polkit	A flaw was found in polkit before version 0.116. The implementation of the polkit_backend_interactive_authority_check_authorization function in polkitd allows to test for authentication and trigger authentication of unrelated processes owned by other users. This may result in a local DoS and information disclosure.
CVE-2019-13232	unzip-6.0-21.el7.x86_64	unzip	Info-ZIP UnZip 6.0 mishandles the overlapping of files inside a ZIP container, leading to denial of service (resource consumption), aka a "better zip bomb" issue.
CVE-2021-27803	wpa_supplicant-2.6-12.el7_9.2.x86_64	wpa_supplicant	A vulnerability was discovered in how p2p/p2p_pd.c in wpa_supplicant before 2.10 processes P2P (Wi-Fi Direct) provision discovery requests. It could result in denial of service or other impact (potentially execution of arbitrary code), for an attacker within radio range.
CVE-2020-12723	perl-5.16.3-299.el7_9.x86_64	perl	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.
CVE-2020-12723	perl-Pod-Escapes-1.04-299.el7_9.noarch	perl-Pod-Escapes	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.
CVE-2020-12723	perl-libs-5.16.3-299.el7_9.x86_64	perl-libs	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.
CVE-2020-12723	perl-macros-5.16.3-299.el7_9.x86_64	perl-macros	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.
CVE-2020-10878	perl-5.16.3-299.el7_9.x86_64	perl	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.
CVE-2020-10878	perl-Pod-Escapes-1.04-299.el7_9.noarch	perl-Pod-Escapes	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.
CVE-2020-10878	perl-libs-5.16.3-299.el7_9.x86_64	perl-libs	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.
CVE-2020-10878	perl-macros-5.16.3-299.el7_9.x86_64	perl-macros	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.
CVE-2020-10543	perl-5.16.3-299.el7_9.x86_64	perl	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
CVE-2020-10543	perl-Pod-Escapes-1.04-299.el7_9.noarch	perl-Pod-Escapes	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.

CVE-2020-10543	perl-libs-5.16.3-299.el7_9.x86_64	perl-libs	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
CVE-2020-10543	perl-macros-5.16.3-299.el7_9.x86_64	perl-macros	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
CVE-2019-16056	python-2.7.5-90.el7.x86_64	python	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.
CVE-2019-16056	python-libs-2.7.5-90.el7.x86_64	python-libs	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.
CVE-2019-16056	python3-3.6.8-18.el7.x86_64	python3	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.
CVE-2019-16056	python3-libs-3.6.8-18.el7.x86_64	python3-libs	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.
CVE-2019-16935	python-2.7.5-90.el7.x86_64	python	The documentation XML-RPC server in Python through 2.7.16, 3.x through 3.6.9, and 3.7.x through 3.7.4 has XSS via the server_title field. This occurs in Lib/DocXMLRPCServer.py in Python 2.x, and in Lib/xmlrpc/server.py in Python 3.x. If set_server_title is called with untrusted input, arbitrary JavaScript can be delivered to clients that visit the http URL for this server.
CVE-2019-16935	python-libs-2.7.5-90.el7.x86_64	python-libs	The documentation XML-RPC server in Python through 2.7.16, 3.x through 3.6.9, and 3.7.x through 3.7.4 has XSS via the server_title field. This occurs in Lib/DocXMLRPCServer.py in Python 2.x, and in Lib/xmlrpc/server.py in Python 3.x. If set_server_title is called with untrusted input, arbitrary JavaScript can be delivered to clients that visit the http URL for this server.
CVE-2019-16935	python3-3.6.8-18.el7.x86_64	python3	The documentation XML-RPC server in Python through 2.7.16, 3.x through 3.6.9, and 3.7.x through 3.7.4 has XSS via the server_title field. This occurs in Lib/DocXMLRPCServer.py in Python 2.x, and in Lib/xmlrpc/server.py in Python 3.x. If set_server_title is called with untrusted input, arbitrary JavaScript can be delivered to clients that visit the http URL for this server.
CVE-2019-16935	python3-libs-3.6.8-18.el7.x86_64	python3-libs	The documentation XML-RPC server in Python through 2.7.16, 3.x through 3.6.9, and 3.7.x through 3.7.4 has XSS via the server_title field. This occurs in Lib/DocXMLRPCServer.py in Python 2.x, and in Lib/xmlrpc/server.py in Python 3.x. If set_server_title is called with untrusted input, arbitrary JavaScript can be delivered to clients that visit the http URL for this server.
CVE-2018-20852	python-2.7.5-90.el7.x86_64	python	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.
CVE-2018-20852	python-libs-2.7.5-90.el7.x86_64	python-libs	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.
CVE-2018-20852	python3-3.6.8-18.el7.x86_64	python3	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.
CVE-2018-20852	python3-libs-3.6.8-18.el7.x86_64	python3-libs	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.
CVE-2019-20907	python-2.7.5-90.el7.x86_64	python	In Lib/tarfile.py in Python through 3.8.3, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation.
CVE-2019-20907	python-libs-2.7.5-90.el7.x86_64	python-libs	In Lib/tarfile.py in Python through 3.8.3, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation.
CVE-2019-20907	python3-3.6.8-18.el7.x86_64	python3	In Lib/tarfile.py in Python through 3.8.3, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation.
CVE-2019-20907	python3-libs-3.6.8-18.el7.x86_64	python3-libs	In Lib/tarfile.py in Python through 3.8.3, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation.
CVE-2020-14422	python3-3.6.8-18.el7.x86_64	python3	Lib/ipaddress.py in Python through 3.8.3 improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created. This is fixed in: v3.5.10, v3.5.10rc1; v3.6.12; v3.7.9; v3.8.4, v3.8.4rc1, v3.8.5, v3.8.6, v3.8.6rc1; v3.9.0, v3.9.0b4, v3.9.0b5, v3.9.0rc1, v3.9.0rc2.
CVE-2020-14422	python3-libs-3.6.8-18.el7.x86_64	python3-libs	Lib/ipaddress.py in Python through 3.8.3 improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created. This is fixed in: v3.5.10, v3.5.10rc1; v3.6.12; v3.7.9; v3.8.4, v3.8.4rc1, v3.8.5, v3.8.6, v3.8.6rc1; v3.9.0, v3.9.0b4, v3.9.0b5, v3.9.0rc1, v3.9.0rc2.
CVE-2020-8492	python3-3.6.8-18.el7.x86_64	python3	Python 2.7 through 2.7.17, 3.5 through 3.5.9, 3.6 through 3.6.10, 3.7 through 3.7.6, and 3.8 through 3.8.1 allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking.
CVE-2020-8492	python3-libs-3.6.8-18.el7.x86_64	python3-libs	Python 2.7 through 2.7.17, 3.5 through 3.5.9, 3.6 through 3.6.10, 3.7 through 3.7.6, and 3.8 through 3.8.1 allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking.
CVE-2019-11236	python3-pip-9.0.3-8.el7.noarch	python3-pip	In the urllib3 library through 1.24.1 for Python, CRLF injection is possible if the attacker controls the request parameter.

CVE-2018-20060	python3-pip-9.0.3-8.el7.noarch	python3-pip	urllib3 before version 1.23 does not remove the Authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or scheme). This can allow for credentials in the Authorization header to be exposed to unintended hosts or transmitted in cleartext.
CVE-2019-11324	python3-pip-9.0.3-8.el7.noarch	python3-pip	The urllib3 library before 1.24.2 for Python mishandles certain cases where the desired set of CA certificates is different from the OS store of CA certificates, which results in SSL connections succeeding in situations where a verification failure is the correct outcome. This is related to use of the ssl_context, ca_certs, or ca_certs_dir argument.
CVE-2018-18074	python3-pip-9.0.3-8.el7.noarch	python3-pip	The Requests package before 2.20.0 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.
CVE-2021-26937	screen-4.1.0-0.27.20120314git3c2946.el7_9.x86_64	screen	encoding.c in GNU Screen through 4.8.0 allows remote attackers to cause a denial of service (invalid write access and application crash) or possibly have unspecified other impact via a crafted UTF-8 character sequence.
CVE-2019-13734	sqlite-3.7.17-8.el7_7.1.x86_64	sqlite	Out of bounds write in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-3156	sudo-1.8.23-10.el7_9.1.x86_64	sudo	Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.

Packages Updated for Security Reasons

Old Package	New Package for CVE
NetworkManager-1.18.0-5.el7.x86_64	NetworkManager-1.18.8-2.el7_9.x86_64
NetworkManager-libnm-1.18.0-5.el7.x86_64	NetworkManager-libnm-1.18.8-2.el7_9.x86_64
NetworkManager-team-1.18.0-5.el7.x86_64	NetworkManager-team-1.18.8-2.el7_9.x86_64
NetworkManager-tui-1.18.0-5.el7.x86_64	NetworkManager-tui-1.18.8-2.el7_9.x86_64
avahi-libs-0.6.31-19.el7.x86_64	avahi-libs-0.6.31-20.el7.x86_64
cpio-2.11-27.el7.x86_64	cpio-2.11-28.el7.x86_64
cups-client-1.6.3-40.el7.x86_64	cups-client-1.6.3-51.el7.x86_64
cups-libs-1.6.3-40.el7.x86_64	cups-libs-1.6.3-51.el7.x86_64
curl-7.29.0-59.el7.x86_64	curl-7.29.0-59.el7_9.1.x86_64
dbus-1.10.24-13.el7_6.x86_64	dbus-1.10.24-15.el7.x86_64
dbus-libs-1.10.24-13.el7_6.x86_64	dbus-libs-1.10.24-15.el7.x86_64
e2fsprogs-1.42.9-16.el7.x86_64	e2fsprogs-1.42.9-19.el7.x86_64
e2fsprogs-libs-1.42.9-16.el7.x86_64	e2fsprogs-libs-1.42.9-19.el7.x86_64
file-5.11-35.el7.x86_64	file-5.11-37.el7.x86_64
file-libs-5.11-35.el7.x86_64	file-libs-5.11-37.el7.x86_64
freetype-2.8-14.el7.x86_64	freetype-2.8-14.el7_9.1.x86_64
fribidi-1.0.2-1.el7.x86_64	fribidi-1.0.2-1.el7_7.1.x86_64
glib2-2.56.1-7.el7.x86_64	glib2-2.56.1-9.el7_9.x86_64
glib2-devel-2.56.1-7.el7.x86_64	glib2-devel-2.56.1-9.el7_9.x86_64
glibc-2.17-292.el7.x86_64	glibc-2.17-323.el7_9.x86_64
glibc-common-2.17-292.el7.x86_64	glibc-common-2.17-323.el7_9.x86_64
grub2-2.02-0.80.el7.centos.x86_64	grub2-2.02-0.87.el7.centos.6.x86_64
grub2-common-2.02-0.80.el7.centos.noarch	grub2-common-2.02-0.87.el7.centos.6.noarch
grub2-pc-2.02-0.80.el7.centos.x86_64	grub2-pc-2.02-0.87.el7.centos.6.x86_64
grub2-pc-modules-2.02-0.80.el7.centos.noarch	grub2-pc-modules-2.02-0.87.el7.centos.6.noarch
grub2-tools-2.02-0.80.el7.centos.x86_64	grub2-tools-2.02-0.87.el7.centos.6.x86_64
grub2-tools-extra-2.02-0.80.el7.centos.x86_64	grub2-tools-extra-2.02-0.87.el7.centos.6.x86_64
grub2-tools-minimal-2.02-0.80.el7.centos.x86_64	grub2-tools-minimal-2.02-0.87.el7.centos.6.x86_64
initscripts-9.49.47-1.el7.x86_64	initscripts-9.49.53-1.el7_9.1.x86_64
ip4r96-2.1-1.rhel7.x86_64	ip4r13-2.4.1-1.rhel7.1.x86_64

java-1.8.0-openjdk-headless-1.8.0.252.b09-2.el7_8.x86_64	java-1.8.0-openjdk-headless-1.8.0.292.b10-1.el7_9.x86_64
kernel-3.10.0-1160.6.1.el7.x86_64	kernel-3.10.0-1160.31.1.el7.x86_64
kernel-devel-3.10.0-1160.6.1.el7.x86_64	kernel-devel-3.10.0-1160.31.1.el7.x86_64
kernel-tools-3.10.0-1160.6.1.el7.x86_64	kernel-tools-3.10.0-1160.31.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.6.1.el7.x86_64	kernel-tools-libs-3.10.0-1160.31.1.el7.x86_64
libX11-1.6.7-2.el7.x86_64	libX11-1.6.7-3.el7_9.x86_64
libX11-common-1.6.7-2.el7.noarch	libX11-common-1.6.7-3.el7_9.noarch
libcom_err-1.42.9-16.el7.x86_64	libcom_err-1.42.9-19.el7.x86_64
libcom_err-devel-1.42.9-16.el7.x86_64	libcom_err-devel-1.42.9-19.el7.x86_64
libcroco-0.6.12-4.el7.x86_64	libcroco-0.6.12-6.el7_9.x86_64
libcurl-7.29.0-59.el7.x86_64	libcurl-7.29.0-59.el7_9.1.x86_64
libicu-50.2-3.el7.x86_64	libicu-50.2-4.el7_7.x86_64
libldb-1.4.2-1.el7.x86_64	libldb-1.5.4-2.el7.x86_64
libmspack-0.5-0.7.alpha.el7.x86_64	libmspack-0.5-0.8.alpha.el7.x86_64
libss-1.42.9-16.el7.x86_64	libss-1.42.9-19.el7.x86_64
libssh2-1.8.0-3.el7.x86_64	libssh2-1.8.0-4.el7.x86_64
libtalloc-2.1.14-1.el7.x86_64	libtalloc-2.1.16-1.el7.x86_64
libtdb-1.3.16-1.el7.x86_64	libtdb-1.3.18-1.el7.x86_64
libtevent-0.9.37-1.el7.x86_64	libtevent-0.9.39-1.el7.x86_64
libwbclient-4.9.1-6.el7.x86_64	libwbclient-4.10.16-15.el7_9.x86_64
libxml2-2.9.1-6.el7_2.3.x86_64	libxml2-2.9.1-6.el7.5.x86_64
libxml2-python-2.9.1-6.el7_2.3.x86_64	libxml2-python-2.9.1-6.el7.5.x86_64
mariadb-libs-5.5.64-1.el7.x86_64	mariadb-libs-5.5.68-1.el7.x86_64
microcode_ctl-2.1-53.el7.x86_64	microcode_ctl-2.1-73.8.el7_9.x86_64
net-snmp-5.7.2-43.el7.x86_64	net-snmp-5.7.2-49.el7_9.1.x86_64
net-snmp-agent-libs-5.7.2-43.el7.x86_64	net-snmp-agent-libs-5.7.2-49.el7_9.1.x86_64
net-snmp-libs-5.7.2-43.el7.x86_64	net-snmp-libs-5.7.2-49.el7_9.1.x86_64
net-snmp-perl-5.7.2-43.el7.x86_64	net-snmp-perl-5.7.2-49.el7_9.1.x86_64
net-snmp-utils-5.7.2-43.el7.x86_64	net-snmp-utils-5.7.2-49.el7_9.1.x86_64
ntp-4.2.6p5-29.el7.centos.x86_64	ntp-4.2.6p5-29.el7.centos.2.x86_64
ntpdate-4.2.6p5-29.el7.centos.x86_64	ntpdate-4.2.6p5-29.el7.centos.2.x86_64
openldap-2.4.44-21.el7_6.x86_64	openldap-2.4.44-23.el7_9.x86_64
openssl-1.0.2k-19.el7.x86_64	openssl-1.0.2k-21.el7_9.x86_64
openssl-libs-1.0.2k-19.el7.x86_64	openssl-libs-1.0.2k-21.el7_9.x86_64
perf-3.10.0-1160.6.1.el7.x86_64	perf-3.10.0-1160.31.1.el7.x86_64
perl-5.16.3-294.el7_6.x86_64	perl-5.16.3-299.el7_9.x86_64
perl-Pod-Escapes-1.04-294.el7_6.noarch	perl-Pod-Escapes-1.04-299.el7_9.noarch
perl-libs-5.16.3-294.el7_6.x86_64	perl-libs-5.16.3-299.el7_9.x86_64
perl-macros-5.16.3-294.el7_6.x86_64	perl-macros-5.16.3-299.el7_9.x86_64
pgaudit11_96-1.1.1-1.rhel7.x86_64	pgaudit15_13-1.5.0-1.rhel7.x86_64
polkit-0.112-22.el7.x86_64	polkit-0.112-26.el7.x86_64
postgresql96-9.6.17-1PGDG.rhel7.x86_64	postgresql13-13.2-1PGDG.rhel7.x86_64
postgresql96-contrib-9.6.17-1PGDG.rhel7.x86_64	postgresql13-contrib-13.2-1PGDG.rhel7.x86_64
postgresql96-libs-9.6.17-1PGDG.rhel7.x86_64	postgresql13-libs-13.2-1PGDG.rhel7.x86_64
postgresql96-plpython-9.6.17-1PGDG.rhel7.x86_64	postgresql13-llvmjit-13.2-1PGDG.rhel7.x86_64
postgresql96-plpython3-9.6.17-1PGDG.rhel7.x86_64	postgresql13-plpython3-13.2-1PGDG.rhel7.x86_64

postgresql96-server-9.6.17-1PGDG.rhel7.x86_64	postgresql13-server-13.2-1PGDG.rhel7.x86_64
pytalloc-2.1.14-1.el7.x86_64	pytalloc-2.1.16-1.el7.x86_64
python-2.7.5-86.el7.x86_64	python-2.7.5-90.el7.x86_64
python-libs-2.7.5-86.el7.x86_64	python-libs-2.7.5-90.el7.x86_64
python3-3.6.8-10.el7.x86_64	python3-3.6.8-18.el7.x86_64
python3-libs-3.6.8-10.el7.x86_64	python3-libs-3.6.8-18.el7.x86_64
python3-pip-9.0.3-5.el7.noarch	python3-pip-9.0.3-8.el7.noarch
rpm-4.11.3-40.el7.x86_64	rpm-4.11.3-45.el7.x86_64
rpm-build-libs-4.11.3-40.el7.x86_64	rpm-build-libs-4.11.3-45.el7.x86_64
rpm-libs-4.11.3-40.el7.x86_64	rpm-libs-4.11.3-45.el7.x86_64
rpm-python-4.11.3-40.el7.x86_64	rpm-python-4.11.3-45.el7.x86_64
samba-4.9.1-6.el7.x86_64	samba-4.10.16-15.el7_9.x86_64
samba-client-libs-4.9.1-6.el7.x86_64	samba-client-libs-4.10.16-15.el7_9.x86_64
samba-common-4.9.1-6.el7.noarch	samba-common-4.10.16-15.el7_9.noarch
samba-common-libs-4.9.1-6.el7.x86_64	samba-common-libs-4.10.16-15.el7_9.x86_64
samba-common-tools-4.9.1-6.el7.x86_64	samba-common-tools-4.10.16-15.el7_9.x86_64
samba-libs-4.9.1-6.el7.x86_64	samba-libs-4.10.16-15.el7_9.x86_64
samba-winbind-4.9.1-6.el7.x86_64	samba-winbind-4.10.16-15.el7_9.x86_64
samba-winbind-clients-4.9.1-6.el7.x86_64	samba-winbind-clients-4.10.16-15.el7_9.x86_64
samba-winbind-modules-4.9.1-6.el7.x86_64	samba-winbind-modules-4.10.16-15.el7_9.x86_64
screen-4.1.0-0.25.20120314git3c2946.el7.x86_64	screen-4.1.0-0.27.20120314git3c2946.el7_9.x86_64
shared-mime-info-1.8-4.el7.x86_64	shared-mime-info-1.8-5.el7.x86_64
sqlite-3.7.17-8.el7.x86_64	sqlite-3.7.17-8.el7_7.1.x86_64
sudo-1.8.23-9.el7.x86_64	sudo-1.8.23-10.el7_9.1.x86_64
systemd-219-73.el7_8.9.x86_64	systemd-219-78.el7_9.3.x86_64
systemd-libs-219-73.el7_8.9.x86_64	systemd-libs-219-78.el7_9.3.x86_64
systemd-python-219-73.el7_8.9.x86_64	systemd-python-219-78.el7_9.3.x86_64
systemd-sysv-219-73.el7_8.9.x86_64	systemd-sysv-219-78.el7_9.3.x86_64
tzdata-java-2019b-1.el7.noarch	tzdata-java-2021a-1.el7.noarch
unzip-6.0-20.el7.x86_64	unzip-6.0-21.el7.x86_64
wpa_supplicant-2.6-12.el7.x86_64	wpa_supplicant-2.6-12.el7_9.2.x86_64
zlib-1.2.7-18.el7.x86_64	zlib-1.2.7-19.el7_9.x86_64

Packages Updated NOT for Security Reasons

Old Package	New Package NOT for CVE
esi-release-4.1.0.0-33786.5469.x86_64	esi-release-4.3.0.0-35578.6185.x86_64
logbase-ui-4.1.0.0-20201216205957.x86_64	logbase-ui-4.3.0.0-20210908174753.x86_64
lumeta-api-4.1.0.0-33784.x86_64	lumeta-api-4.3.0.0-35571.x86_64
lumeta-api-client-4.1.0.0-31980.x86_64	lumeta-api-client-4.3.0.0-35517.x86_64
lumeta-cisco-ise-pxgrid-4.0.0.0-31455.x86_64	lumeta-cisco-ise-pxgrid-4.3.0.0-31455.x86_64
lumeta-console-4.1.0.0-33433.x86_64	lumeta-console-4.3.0.0-35437.x86_64
lumeta-diagnostics-4.1.0.0-33556.x86_64	lumeta-diagnostics-4.3.0.0-35301.x86_64
lumeta-discovery-agent-4.1.0.0-33421.x86_64	lumeta-discovery-agent-4.3.0.0-35569.x86_64
lumeta-dxl-4.1.0.0-33714.x86_64	lumeta-dxl-4.3.0.0-34658.x86_64
lumeta-install-4.1.0.0-33668.x86_64	lumeta-install-4.3.0.0-35577.x86_64

lumeta-ips-import-4.0.0.0-30573.x86_64	lumeta-ips-import-4.3.0.0-30740.x86_64
lumeta-ireg-4.1.0.0-6550.x86_64	lumeta-ireg-4.3.0.0-6550.x86_64
lumeta-lib-4.1.0.0-32781.x86_64	lumeta-lib-4.3.0.0-35480.x86_64
lumeta-pam-4.0.0.0-31405.x86_64	lumeta-pam-4.3.0.0-34789.x86_64
lumeta-tools-3.3.3.0-10695.x86_64	lumeta-tools-4.3.0.0-34180.x86_64
lumeta-ui-4.1.0.0-33603.x86_64	lumeta-ui-4.3.0.0-35247.x86_64
lumeta-visio-3.3.3.0-12259.x86_64	lumeta-visio-4.3.0.0-34789.x86_64
lumeta-warehouse-4.1.0.0-33769.x86_64	lumeta-warehouse-4.3.0.0-35421.x86_64
lumeta-webapp-4.1.0.0-33552.x86_64	lumeta-webapp-4.3.0.0-35385.x86_64
rawio-3.3.3.0-8288.x86_64	rawio-4.3.0.0-30699.x86_64

New Packages

New Packages
GeoIP-1.5.0-14.el7.x86_64
bind-libs-9.11.4-9.P2.el7.x86_64
bind-libs-lite-9.11.4-9.P2.el7.x86_64
bind-license-9.11.4-9.P2.el7.noarch
bind-utils-9.11.4-9.P2.el7.x86_64
elfutils-devel-0.176-2.el7.x86_64
elfutils-libelf-devel-0.176-2.el7.x86_64
gdbm-devel-1.10-8.el7.x86_64
geoipupdate-2.5.0-1.el7.x86_64
glibc-devel-2.17-323.el7_9.x86_64
glibc-headers-2.17-323.el7_9.x86_64
gnutls-3.3.29-9.el7_6.x86_64
jq-1.6-2.el7.x86_64
kernel-headers-3.10.0-1160.31.1.el7.x86_64
libdb-devel-5.3.21-25.el7.x86_64
llvm5.0-5.0.1-7.el7.x86_64
llvm5.0-libs-5.0.1-7.el7.x86_64
lm_sensors-devel-3.4.0-8.20160601gitf9185e5.el7. x86_64
net-snmp-devel-5.7.2-49.el7_9.1.x86_64
nettle-2.7.1-9.el7_9.x86_64
nscd-2.17-323.el7_9.x86_64
nss-pam-ldapd-0.8.13-16.el7_6.1.x86_64
oniguruma-6.8.2-1.el7.x86_64
openldap-clients-2.4.44-23.el7_9.x86_64
openssl-devel-1.0.2k-21.el7_9.x86_64
perl-ExtUtils-Install-1.58-299.el7_9.noarch
perl-ExtUtils-MakeMaker-6.68-3.el7.noarch
perl-ExtUtils-Manifest-1.61-244.el7.noarch

perl-ExtUtils-ParseXS-3.18-3.el7.noarch
perl-Test-Harness-3.28-3.el7.noarch
perl-devel-5.16.3-299.el7_9.x86_64
popt-devel-1.13-16.el7.x86_64
pyldb-1.5.4-2.el7.x86_64
pyparsing-1.5.6-9.el7.noarch
systemtap-sdt-devel-4.0-9.el7.x86_64
tcp_wrappers-devel-7.6-77.el7.x86_64
trousers-0.3.14-2.el7.x86_64
virt-what-1.18-4.el7.x86_64
xz-devel-5.2.2-1.el7.x86_64
zlib-devel-1.2.7-19.el7_9.x86_64
python-tdb-1.3.18-1.el7.x86_64
rpm-devel-4.11.3-45.el7.x86_64

Packages Updated NOT for Security Reasons

Old Packaage	New Package NOT for CVE
esi-release-4.1.0.0-33786.5469.x86_64	esi-release-4.3.0.0-35445.6141.x86_64
logbase-ui-4.1.0.0-20201216205957.x86_64	logbase-ui-4.3.0.0a20210820184747.x86_64
lumeta-api-4.1.0.0-33784.x86_64	lumeta-api-4.3.0.0-35444.x86_64
lumeta-api-client-4.1.0.0-31980.x86_64	lumeta-api-client-4.3.0.0-35385.x86_64
lumeta-cisco-ise-pxgrid-4.0.0.0-31455.x86_64	lumeta-cisco-ise-pxgrid-4.3.0.0-31455.x86_64
lumeta-console-4.1.0.0-33433.x86_64	lumeta-console-4.3.0.0-35437.x86_64
lumeta-diagnostics-4.1.0.0-33556.x86_64	lumeta-diagnostics-4.3.0.0-35301.x86_64
lumeta-discovery-agent-4.1.0.0-33421.x86_64	lumeta-discovery-agent-4.3.0.0-35396.x86_64
lumeta-dxl-4.1.0.0-33714.x86_64	lumeta-dxl-4.3.0.0-34658.x86_64
lumeta-install-4.1.0.0-33668.x86_64	lumeta-install-4.3.0.0-35442.x86_64
lumeta-ips-import-4.0.0.0-30573.x86_64	lumeta-ips-import-4.3.0.0-30740.x86_64
lumeta-ireg-4.1.0.0-6550.x86_64	lumeta-ireg-4.3.0.0-6550.x86_64
lumeta-lib-4.1.0.0-32781.x86_64	lumeta-lib-4.3.0.0-35220.x86_64
lumeta-pam-4.0.0.0-31405.x86_64	lumeta-pam-4.3.0.0-34789.x86_64
lumeta-tools-3.3.3.0-10695.x86_64	lumeta-tools-4.3.0.0-34180.x86_64
lumeta-ui-4.1.0.0-33603.x86_64	lumeta-ui-4.3.0.0-35247.x86_64
lumeta-visio-3.3.3.0-12259.x86_64	lumeta-visio-4.3.0.0-34789.x86_64
lumeta-warehouse-4.1.0.0-33769.x86_64	lumeta-warehouse-4.3.0.0-35421.x86_64
lumeta-webapp-4.1.0.0-33552.x86_64	lumeta-webapp-4.3.0.0-35385.x86_64

Removed Packages

Removed Packages
python-jsonpath-rw-1.2.3-2.el7.noarch

python-ply-3.4-11.el7.noarch
python-six-1.9.0-2.el7.noarch
python36-decorator-4.0.11-2.el7.noarch
python36-ply-3.9-2.el7.noarch
python36-six-1.14.0-2.el7.noarch