Security Advisories 4.6

This page shows the package changes from 4.5 to 4.6 some for security reasons and the CVEs.

Deliverable	Name
netboot	esi-4.6

CVE-2021-4083	kernel-3.10.0-1160.76.1.el7.x86_64	kernel	A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system. This flaw affects Linux kernel versions prior to 5.16-rc4.
CVE-2021-4083	kernel-devel-3.10.0-1160.76.1.el7.x86_64	kernel-devel	A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system. This flaw affects Linux kernel versions prior to 5.16-rc4.
CVE-2021-4083	kernel-headers-3.10.0-1160.76.1.el7.x86_64	kernel-headers	A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system. This flaw affects Linux kernel versions prior to 5.16-rc4.
CVE-2021-4083	kernel-tools-3.10.0-1160.76.1.el7.x86_64	kernel-tools	A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system. This flaw affects Linux kernel versions prior to 5.16-rc4.
CVE-2021-4083	kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64	kernel-tools-libs	A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system. This flaw affects Linux kernel versions prior to 5.16-rc4.
CVE-2021-4083	perf-3.10.0-1160.76.1.el7.x86_64	perf	A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system. This flaw affects Linux kernel versions prior to 5.16-rc4.
CVE-2022-1966	kernel-3.10.0-1160.76.1.el7.x86_64	kernel	DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-32250. Reason: This candidate is a duplicate of CVE-2022-32250. Notes: All CVE users should reference CVE-2022-32250 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2022-1966	kernel-devel-3.10.0-1160.76.1.el7.x86_64	kernel-devel	DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-32250. Reason: This candidate is a duplicate of CVE-2022-32250. Notes: All CVE users should reference CVE-2022-32250 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2022-1966	kernel-headers-3.10.0-1160.76.1.el7.x86_64	kernel-headers	DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-32250. Reason: This candidate is a duplicate of CVE-2022-32250. Notes: All CVE users should reference CVE-2022-32250 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2022-1966	kernel-tools-3.10.0-1160.76.1.el7.x86_64	kernel-tools	DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-32250. Reason: This candidate is a duplicate of CVE-2022-32250. Notes: All CVE users should reference CVE-2022-32250 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2022-1966	kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64	kernel-tools-libs	DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-32250. Reason: This candidate is a duplicate of CVE-2022-32250. Notes: All CVE users should reference CVE-2022-32250 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2022-1966	perf-3.10.0-1160.76.1.el7.x86_64	perf	DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-32250. Reason: This candidate is a duplicate of CVE-2022-32250. Notes: All CVE users should reference CVE-2022-32250 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.

CVE-2022-21125	kernel-3.10.0-1160.76.1.el7.x86_64	kernel	Incomplete cleanup of microarchitectural fill buffers on some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21125	kernel-devel-3.10.0-1160.76.1.el7.x86_64	kernel-devel	Incomplete cleanup of microarchitectural fill buffers on some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21125	kernel-headers-3.10.0-1160.76.1.el7.x86_64	kernel-headers	Incomplete cleanup of microarchitectural fill buffers on some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21125	kernel-tools-3.10.0-1160.76.1.el7.x86_64	kernel-tools	Incomplete cleanup of microarchitectural fill buffers on some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21125	kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64	kernel-tools-libs	Incomplete cleanup of microarchitectural fill buffers on some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21125	perf-3.10.0-1160.76.1.el7.x86_64	perf	Incomplete cleanup of microarchitectural fill buffers on some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21166	kernel-3.10.0-1160.76.1.el7.x86_64	kernel	Incomplete cleanup in specific special register write operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21166	kernel-devel-3.10.0-1160.76.1.el7.x86_64	kernel-devel	Incomplete cleanup in specific special register write operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21166	kernel-headers-3.10.0-1160.76.1.el7.x86_64	kernel-headers	Incomplete cleanup in specific special register write operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21166	kernel-tools-3.10.0-1160.76.1.el7.x86_64	kernel-tools	Incomplete cleanup in specific special register write operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21166	kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64	kernel-tools-libs	Incomplete cleanup in specific special register write operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21166	perf-3.10.0-1160.76.1.el7.x86_64	perf	Incomplete cleanup in specific special register write operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2021-4028	kernel-3.10.0-1160.76.1.el7.x86_64	kernel	A flaw in the Linux kernel's implementation of RDMA communications manager listener code allowed an attacker with local access to setup a socket to listen on a high port allowing for a list element to be used after free. Given the ability to execute code, a local attacker could leverage this use-after-free to crash the system or possibly escalate privileges on the system.

CVE-2021-4028	kernel-devel-3.10.0-1160.76.1.el7.x86_64	kernel-devel	A flaw in the Linux kernel's implementation of RDMA communications manager listener code allowed an attacker with local access to setup a socket to listen on a high port allowing for a list element to be used after free. Given the ability to execute code, a local attacker could leverage this use-after-free to crash the system or possibly escalate privileges on the system.
CVE-2021-4028	kernel-headers-3.10.0-1160.76.1.el7.x86_64	kernel-headers	A flaw in the Linux kernel's implementation of RDMA communications manager listener code allowed an attacker with local access to setup a socket to listen on a high port allowing for a list element to be used after free. Given the ability to execute code, a local attacker could leverage this use-after-free to crash the system or possibly escalate privileges on the system.
CVE-2021-4028	kernel-tools-3.10.0-1160.76.1.el7.x86_64	kernel-tools	A flaw in the Linux kernel's implementation of RDMA communications manager listener code allowed an attacker with local access to setup a socket to listen on a high port allowing for a list element to be used after free. Given the ability to execute code, a local attacker could leverage this use-after-free to crash the system or possibly escalate privileges on the system.
CVE-2021-4028	kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64	kernel-tools-libs	A flaw in the Linux kernel's implementation of RDMA communications manager listener code allowed an attacker with local access to setup a socket to listen on a high port allowing for a list element to be used after free. Given the ability to execute code, a local attacker could leverage this use-after-free to crash the system or possibly escalate privileges on the system.
CVE-2021-4028	perf-3.10.0-1160.76.1.el7.x86_64	perf	A flaw in the Linux kernel's implementation of RDMA communications manager listener code allowed an attacker with local access to setup a socket to listen on a high port allowing for a list element to be used after free. Given the ability to execute code, a local attacker could leverage this use-after-free to crash the system or possibly escalate privileges on the system.
CVE-2022-0492	kernel-3.10.0-1160.76.1.el7.x86_64	kernel	A vulnerability was found in the Linux kernel’s cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.
CVE-2022-0492	kernel-devel-3.10.0-1160.76.1.el7.x86_64	kernel-devel	A vulnerability was found in the Linux kernel’s cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.
CVE-2022-0492	kernel-headers-3.10.0-1160.76.1.el7.x86_64	kernel-headers	A vulnerability was found in the Linux kernel’s cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.
CVE-2022-0492	kernel-tools-3.10.0-1160.76.1.el7.x86_64	kernel-tools	A vulnerability was found in the Linux kernel’s cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.
CVE-2022-0492	kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64	kernel-tools-libs	A vulnerability was found in the Linux kernel’s cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.
CVE-2022-0492	perf-3.10.0-1160.76.1.el7.x86_64	perf	A vulnerability was found in the Linux kernel’s cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.
CVE-2022-21123	kernel-3.10.0-1160.76.1.el7.x86_64	kernel	Incomplete cleanup of multi-core shared buffers for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21123	kernel-devel-3.10.0-1160.76.1.el7.x86_64	kernel-devel	Incomplete cleanup of multi-core shared buffers for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVE-2022-21123	kernel-headers-3.10.0-1160.76.1.el7.x86_64	kernel-headers	Incomplete cleanup of multi-core shared buffers for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21123	kernel-tools-3.10.0-1160.76.1.el7.x86_64	kernel-tools	Incomplete cleanup of multi-core shared buffers for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21123	kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64	kernel-tools-libs	Incomplete cleanup of multi-core shared buffers for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-21123	perf-3.10.0-1160.76.1.el7.x86_64	perf	Incomplete cleanup of multi-core shared buffers for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2021-3177	python-2.7.5-92.el7_9.x86_64	python	Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.
CVE-2021-3177	python-libs-2.7.5-92.el7_9.x86_64	python-libs	Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.
CVE-2020-26116	python-2.7.5-92.el7_9.x86_64	python	http.client in Python 3.x before 3.5.10, 3.6.x before 3.6.12, 3.7.x before 3.7.9, and 3.8.x before 3.8.5 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request.
CVE-2020-26116	python-libs-2.7.5-92.el7_9.x86_64	python-libs	http.client in Python 3.x before 3.5.10, 3.6.x before 3.6.12, 3.7.x before 3.7.9, and 3.8.x before 3.8.5 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request.
CVE-2022-0391	python-2.7.5-92.el7_9.x86_64	python	A flaw was found in Python, specifically within the urllib.parse module. This module helps break Uniform Resource Locator (URL) strings into components. The issue involves how the urlparse method does not sanitize input and allows characters like '\r' and '\n' in the URL path. This flaw allows an attacker to input a crafted URL, leading to injection attacks. This flaw affects Python versions prior to 3.10.0b1, 3.9.5, 3.8.11, 3.7.11 and 3.6.14.
CVE-2022-0391	python-libs-2.7.5-92.el7_9.x86_64	python-libs	A flaw was found in Python, specifically within the urllib.parse module. This module helps break Uniform Resource Locator (URL) strings into components. The issue involves how the urlparse method does not sanitize input and allows characters like '\r' and '\n' in the URL path. This flaw allows an attacker to input a crafted URL, leading to injection attacks. This flaw affects Python versions prior to 3.10.0b1, 3.9.5, 3.8.11, 3.7.11 and 3.6.14.
CVE-2020-26137	python-2.7.5-92.el7_9.x86_64	python	urllib3 before 1.25.9 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of putrequest(). NOTE: this is similar to CVE-2020-26116.
CVE-2020-26137	python-libs-2.7.5-92.el7_9.x86_64	python-libs	urllib3 before 1.25.9 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of putrequest(). NOTE: this is similar to CVE-2020-26116.

Packages Updated for Security Reasons

Old Package	**New Package**

bcc-0.8.0-1.el7.x86_64	bcc-0.10.0-1.el7.x86_64
bcc-tools-0.8.0-1.el7.x86_64	bcc-tools-0.10.0-1.el7.x86_64
firewalld-0.6.3-2.el7.noarch	firewalld-0.6.3-13.el7_9.noarch
firewalld-filesystem-0.6.3-2.el7.noarch	firewalld-filesystem-0.6.3-13.el7_9.noarch
java-1.8.0-openjdk-headless-1.8.0.312.b07-1.el7_9.x86_64	java-1.8.0-openjdk-headless-1.8.0.342.b07-1.el7_9.x86_64
kernel-3.10.0-1160.59.1.el7.x86_64	kernel-3.10.0-1160.76.1.el7.x86_64
kernel-devel-3.10.0-1160.59.1.el7.x86_64	kernel-devel-3.10.0-1160.76.1.el7.x86_64
kernel-headers-3.10.0-1160.59.1.el7.x86_64	kernel-headers-3.10.0-1160.76.1.el7.x86_64
kernel-tools-3.10.0-1160.59.1.el7.x86_64	kernel-tools-3.10.0-1160.76.1.el7.x86_64
kernel-tools-libs-3.10.0-1160.59.1.el7.x86_64	kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64
perf-3.10.0-1160.59.1.el7.x86_64	perf-3.10.0-1160.76.1.el7.x86_64
python-2.7.5-90.el7.x86_64	python-2.7.5-92.el7_9.x86_64
python-bcc-0.8.0-1.el7.x86_64	python-bcc-0.10.0-1.el7.x86_64
python-firewall-0.6.3-2.el7.noarch	python-firewall-0.6.3-13.el7_9.noarch
python-libs-2.7.5-90.el7.x86_64	python-libs-2.7.5-92.el7_9.x86_64
python-urlgrabber-3.10-9.el7.noarch	python-urlgrabber-3.10-10.el7.noarch
tzdata-2019b-1.el7.noarch	tzdata-2022c-1.el7.noarch
tzdata-java-2021c-1.el7.noarch	tzdata-java-2022c-1.el7.noarch

Packages Updated NOT for Security Reasons

Old Package	New Package NOT for CVE
esi-release-4.5.0.0-37167.17.x86_64	esi-release-4.6.0.0-eb72758.x86_64
logbase-ui-4.5.0.0-20220513131431.x86_64	logbase-ui-4.6.0.0-eb72758.x86_64
lumeta-api-4.5.0.0-37166.x86_64	lumeta-api-4.6.0.0-eb72758.x86_64
lumeta-api-client-4.5.0.0-37079.x86_64	lumeta-api-client-4.6.0.0-7fded31.x86_64
lumeta-api-python-4.5.0.0-36740.x86_64	lumeta-api-python-4.6.0.0-7cf4e01.x86_64
lumeta-console-4.5.0.0-36699.x86_64	lumeta-console-4.6.0.0-7cf4e01.x86_64
lumeta-diagnostics-4.5.0.0-37053.x86_64	lumeta-diagnostics-4.6.0.0-7cf4e01.x86_64
lumeta-discovery-agent-4.5.0.0-37124.x86_64	lumeta-discovery-agent-4.6.0.0-7cf4e01.x86_64
lumeta-install-4.5.0.0-36999.x86_64	lumeta-install-4.6.0.0-ba85dee.x86_64
lumeta-ips-import-4.5.0.0-36617.x86_64	lumeta-ips-import-4.6.0.0-7cf4e01.x86_64
lumeta-ireg-4.5.0.0-6550.x86_64	lumeta-ireg-4.6.0.0-eb72758.x86_64
lumeta-lib-4.5.0.0-36673.x86_64	lumeta-lib-4.6.0.0-eb72758.x86_64
lumeta-pam-4.5.0.0-34789.x86_64	lumeta-pam-4.6.0.0-7cf4e01.x86_64
lumeta-tools-4.5.0.0-37006.x86_64	lumeta-tools-4.6.0.0-7cf4e01.x86_64
lumeta-visio-4.5.0.0-34789.x86_64	lumeta-visio-4.6.0.0-7cf4e01.x86_64
lumeta-warehouse-4.5.0.0-37144.x86_64	lumeta-warehouse-4.6.0.0-7fded31.x86_64
lumeta-webapp-4.5.0.0-37006.x86_64	lumeta-webapp-4.6.0.0-7cf4e01.x86_64
netflow-capture-1.3.6p1-33423.x86_64	netflow-capture-1.3.6p1-7cf4e01.x86_6
rawio-4.5.0.0-36989.x86_64	rawio-4.6.0.0-7cf4e01.x86_64

New Packages

New Packages
None

Removed Packages

Removed Packages
lumeta-cisco-ise-pxgrid-4.5.0.0-37006.x86_64
lumeta-dxl-4.5.0.0-34658.x86_64
lumeta-ui-4.5.0.0-37006.x86_64
python-psycopg2-2.5.1-4.el7.x86_64