Security Advisories 4.4

This page shows the package changes from 4.3 to 4.4 some for security reasons and the CVEs.

Deliverable	Name
upgrade	lumeta_update-4.4.0.0.36479-20220113.tgz

CVEs and the new package and RPM that resolves each

CVE	New RPM	PKG	DESCRIPTION
CVE-2021-31535	libX11-1.6.7-4.el7_9.x86_64	libX11	LookupCol.c in X.Org X through X11R7.7 and libX11 before 1.7.1 might allow remote attackers to execute arbitrary code. The libX11 XLookupColor request (intended for server-side color lookup) contains a flaw allowing a client to send color-name requests with a name longer than the maximum size allowed by the protocol (and also longer than the maximum packet size for normal-sized packets). The user-controlled data exceeding the maximum size is then interpreted by the server as additional X protocol requests and executed, e.g., to disable X server authorization completely. For example, if the victim encounters malicious terminal control sequences for color codes, then the attacker may be able to take full control of the running graphical session.
CVE-2021-31535	libX11-common-1.6.7-4.el7_9.noarch	libX11-common	LookupCol.c in X.Org X through X11R7.7 and libX11 before 1.7.1 might allow remote attackers to execute arbitrary code. The libX11 XLookupColor request (intended for server-side color lookup) contains a flaw allowing a client to send color-name requests with a name longer than the maximum size allowed by the protocol (and also longer than the maximum packet size for normal-sized packets). The user-controlled data exceeding the maximum size is then interpreted by the server as additional X protocol requests and executed, e.g., to disable X server authorization completely. For example, if the victim encounters malicious terminal control sequences for color codes, then the attacker may be able to take full control of the running graphical session.
CVE-2019-20934	kernel-3.10.0-1160.36.2.el7.x86_64	kernel	An issue was discovered in the Linux kernel before 5.2.6. On NUMA systems, the Linux fair scheduler has a use-after-free in show_numa_stats() because NUMA fault statistics are inappropriately freed, aka CID-16d51a590a8c.
CVE-2019-20934	kernel-devel-3.10.0-1160.36.2.el7.x86_64	kernel-devel	An issue was discovered in the Linux kernel before 5.2.6. On NUMA systems, the Linux fair scheduler has a use-after-free in show_numa_stats() because NUMA fault statistics are inappropriately freed, aka CID-16d51a590a8c.
CVE-2019-20934	kernel-headers-3.10.0-1160.36.2.el7.x86_64	kernel-headers	An issue was discovered in the Linux kernel before 5.2.6. On NUMA systems, the Linux fair scheduler has a use-after-free in show_numa_stats() because NUMA fault statistics are inappropriately freed, aka CID-16d51a590a8c.
CVE-2019-20934	kernel-tools-3.10.0-1160.36.2.el7.x86_64	kernel-tools	An issue was discovered in the Linux kernel before 5.2.6. On NUMA systems, the Linux fair scheduler has a use-after-free in show_numa_stats() because NUMA fault statistics are inappropriately freed, aka CID-16d51a590a8c.
CVE-2019-20934	kernel-tools-libs-3.10.0-1160.36.2.el7.x86_64	kernel-tools-libs	An issue was discovered in the Linux kernel before 5.2.6. On NUMA systems, the Linux fair scheduler has a use-after-free in show_numa_stats() because NUMA fault statistics are inappropriately freed, aka CID-16d51a590a8c.
CVE-2019-20934	perf-3.10.0-1160.45.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 5.2.6. On NUMA systems, the Linux fair scheduler has a use-after-free in show_numa_stats() because NUMA fault statistics are inappropriately freed, aka CID-16d51a590a8c.
CVE-2021-33034	kernel-3.10.0-1160.36.2.el7.x86_64	kernel	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.
CVE-2021-33034	kernel-devel-3.10.0-1160.36.2.el7.x86_64	kernel-devel	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.
CVE-2021-33034	kernel-headers-3.10.0-1160.36.2.el7.x86_64	kernel-headers	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.
CVE-2021-33034	kernel-tools-3.10.0-1160.36.2.el7.x86_64	kernel-tools	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.

CVE-2021-33034	kernel-tools-libs-3.10.0-1160.36.2.el7.x86_64	kernel-tools-libs	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.
CVE-2021-33034	perf-3.10.0-1160.45.1.el7.x86_64	perf	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.
CVE-2020-11668	kernel-3.10.0-1160.36.2.el7.x86_64	kernel	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2020-11668	kernel-devel-3.10.0-1160.36.2.el7.x86_64	kernel-devel	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2020-11668	kernel-headers-3.10.0-1160.36.2.el7.x86_64	kernel-headers	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2020-11668	kernel-tools-3.10.0-1160.36.2.el7.x86_64	kernel-tools	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2020-11668	kernel-tools-libs-3.10.0-1160.36.2.el7.x86_64	kernel-tools-libs	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2020-11668	perf-3.10.0-1160.45.1.el7.x86_64	perf	In the Linux kernel before 5.6.1, drivers/media/usb/gspca/xirlink_cit.c (aka the Xirlink camera USB driver) mishandles invalid descriptors, aka CID-a246b4d54770.
CVE-2016-4658	libxml2-2.9.1-6.el7_9.6.x86_64	libxml2	xpointer.c in libxml2 before 2.9.5 (as used in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3, and other products) does not forbid namespace nodes in XPointer ranges, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and memory corruption) via a crafted XML document.
CVE-2016-4658	libxml2-python-2.9.1-6.el7_9.6.x86_64	libxml2-python	xpointer.c in libxml2 before 2.9.5 (as used in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3, and other products) does not forbid namespace nodes in XPointer ranges, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and memory corruption) via a crafted XML document.
CVE-2020-25717	libwbclient-4.10.16-17.el7_9.x86_64	libwbclient	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-25717	samba-4.10.16-17.el7_9.x86_64	samba	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-25717	samba-client-libs-4.10.16-17.el7_9.x86_64	samba-client-libs	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-25717	samba-common-4.10.16-17.el7_9.noarch	samba-common	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-25717	samba-common-libs-4.10.16-17.el7_9.x86_64	samba-common-libs	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2020-25717	samba-common-tools-4.10.16-17.el7_9.x86_64	samba-common-tools	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-25717	samba-libs-4.10.16-17.el7_9.x86_64	samba-libs	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-25717	samba-winbind-4.10.16-17.el7_9.x86_64	samba-winbind	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-25717	samba-winbind-clients-4.10.16-17.el7_9.x86_64	samba-winbind-clients	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-25717	samba-winbind-modules-4.10.16-17.el7_9.x86_64	samba-winbind-modules	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	libwbclient-4.10.16-17.el7_9.x86_64	libwbclient	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	samba-4.10.16-17.el7_9.x86_64	samba	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	samba-client-libs-4.10.16-17.el7_9.x86_64	samba-client-libs	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	samba-common-4.10.16-17.el7_9.noarch	samba-common	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	samba-common-libs-4.10.16-17.el7_9.x86_64	samba-common-libs	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	samba-common-tools-4.10.16-17.el7_9.x86_64	samba-common-tools	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	samba-libs-4.10.16-17.el7_9.x86_64	samba-libs	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	samba-winbind-4.10.16-17.el7_9.x86_64	samba-winbind	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	samba-winbind-clients-4.10.16-17.el7_9.x86_64	samba-winbind-clients	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-2124	samba-winbind-modules-4.10.16-17.el7_9.x86_64	samba-winbind-modules	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2021-43527	nss-3.67.0-4.el7_9.x86_64	nss	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. **Note: This vulnerability does NOT impact Mozilla Firefox.** However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.

CVE-2021-43527	nss-sysinit-3.67.0-4.el7_9.x86_64	nss-sysinit	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. **Note: This vulnerability does NOT impact Mozilla Firefox.** However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.
CVE-2021-43527	nss-tools-3.67.0-4.el7_9.x86_64	nss-tools	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS #7, or PKCS #12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. **Note: This vulnerability does NOT impact Mozilla Firefox.** However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.
CVE-2021-22555	perf-3.10.0-1160.45.1.el7.x86_64	perf	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space
CVE-2021-3656	perf-3.10.0-1160.45.1.el7.x86_64	perf	• • This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2021-37576	perf-3.10.0-1160.45.1.el7.x86_64	perf	arch/powerpc/kvm/book3s_rtas.c in the Linux kernel through 5.13.5 on the powerpc platform allows KVM guest OS users to cause host OS memory corruption via rtas_args.nargs, aka CID-f62f3c20647e.
CVE-2020-27777	perf-3.10.0-1160.45.1.el7.x86_64	perf	A flaw was found in the way RTAS handled memory accesses in userspace to kernel communication. On a locked down (usually due to Secure Boot) guest system running on top of PowerVM or KVM hypervisors (pseries platform) a root like local user could use this flaw to further increase their privileges to that of a running kernel.
CVE-2021-3653	perf-3.10.0-1160.45.1.el7.x86_64	perf	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7.
CVE-2021-29650	perf-3.10.0-1160.45.1.el7.x86_64	perf	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value, aka CID-175e476b8cdf.
CVE-2021-29154	perf-3.10.0-1160.45.1.el7.x86_64	perf	BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch displacements, allowing them to execute arbitrary code within the kernel context. This affects arch/x86/net/bpf_jit_comp.c and arch/x86/net/bpf_jit_comp32.c.

Packages Updated NOT for Security Reasons

Old Package	New Package NOT for CVE
esi-release-4.3.0.0-35578.6185.x86_64	esi-release-4.4.0.0-36479.25.x86_64
logbase-ui-4.3.0.0-20210908174753.x86_64	logbase-ui-4.4.0.0-20220113210713.x86_64
lumeta-api-4.3.0.0-35571.x86_64	lumeta-api-4.4.0.0-36477.x86_64
lumeta-api-client-4.3.0.0-35517.x86_64	lumeta-api-client-4.4.0.0-36002.x86_64
lumeta-cisco-ise-pxgrid-4.3.0.0-31455.x86_64	lumeta-cisco-ise-pxgrid-4.4.0.0-31455.x86_64
lumeta-console-4.3.0.0-35437.x86_64	lumeta-console-4.4.0.0-36225.x86_64
lumeta-diagnostics-4.3.0.0-35301.x86_64	lumeta-diagnostics-4.4.0.0-35301.x86_64
lumeta-discovery-agent-4.3.0.0-35569.x86_64	lumeta-discovery-agent-4.4.0.0-36247.x86_64
lumeta-dxl-4.3.0.0-34658.x86_64	lumeta-dxl-4.4.0.0-34658.x86_64
lumeta-install-4.3.0.0-35577.x86_64	lumeta-install-4.4.0.0-36339.x86_64
lumeta-ips-import-4.3.0.0-30740.x86_64	lumeta-ips-import-4.4.0.0-36334.x86_64
lumeta-ireg-4.3.0.0-6550.x86_64	lumeta-ireg-4.4.0.0-6550.x86_64
lumeta-lib-4.3.0.0-35480.x86_64	lumeta-lib-4.4.0.0-36203.x86_64
lumeta-pam-4.3.0.0-34789.x86_64	lumeta-pam-4.4.0.0-34789.x86_64
lumeta-tools-4.3.0.0-34180.x86_64	lumeta-tools-4.4.0.0-35385.x86_64
lumeta-ui-4.3.0.0-35247.x86_64	lumeta-ui-4.4.0.0-36238.x86_64

lumeta-visio-4.3.0.0-34789.x86_64	lumeta-visio-4.4.0.0-34789.x86_64
lumeta-warehouse-4.3.0.0-35421.x86_64	lumeta-warehouse-4.4.0.0-36429.x86_64
lumeta-webapp-4.3.0.0-35385.x86_64	lumeta-webapp-4.4.0.0-35919.x86_64

New Packages

New Packages
None

Removed Packages

Removed Packages
None