CVEs Fixed in Lumeta 3.3.2.2

Lumeta continually corrects for Common Vulnerabilities & Exposures (CVEs) in our software products. Following is the finalized list of CVEs mitigated in preparation for the release of Lumeta 3.3.2.2.

Upgrade to 3.3.2.2 is allowed form 3.3.2 and 3.3.2.1. This page shows the diffs only from 3.3.2 to 3.3.2.2.

Deliverable	Name
netboot	esi-3.3.2.2
upgrade	spectre_update-3.3.2.2.13174-20190220.tgz

CVEs and the new package and RPM that resolves each from 3.3.2 to 3.3.2.2.

CVE	New RPM	PKG	DESCRIPTION
CVE-2018-14634	kernel-2.6.32-754.6.3.el6.x86_64	kernel	An integer overflow flaw was found in the Linux kernel'screate_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.
CVE-2018-14634	kernel-firmware-2.6.32-754.6.3.el6.noarch	kernel-firmware	An integer overflow flaw was found in the Linux kernel'screate_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.
CVE-2018-14634	kernel-headers-2.6.32-754.6.3.el6.x86_64	kernel-headers	An integer overflow flaw was found in the Linux kernel'screate_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.
CVE-2018-14634	perf-2.6.32-754.6.3.el6.x86_64	perf	An integer overflow flaw was found in the Linux kernel'screate_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.
CVE-2018-5391	kernel-2.6.32-754.6.3.el6.x86_64	kernel	The Linux kernel, versions 3.9+, is vulnerable to a denial of serviceattack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.
CVE-2018-5391	kernel-firmware-2.6.32-754.6.3.el6.noarch	kernel-firmware	The Linux kernel, versions 3.9+, is vulnerable to a denial of serviceattack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.
CVE-2018-5391	kernel-headers-2.6.32-754.6.3.el6.x86_64	kernel-headers	The Linux kernel, versions 3.9+, is vulnerable to a denial of serviceattack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.
CVE-2018-5391	perf-2.6.32-754.6.3.el6.x86_64	perf	The Linux kernel, versions 3.9+, is vulnerable to a denial of serviceattack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.
CVE-2018-12327	ntp-4.2.6p5-15.el6.centos.x86_64	ntp	Stack-based buffer overflow in ntpq and ntpdc of NTP version 4.2.8p11allows an attacker to achieve code execution or escalate to higher privileges via a long string as the argument for an IPv4 or IPv6 command-line parameter. NOTE: It is unclear whether there are any common situations in which ntpq or ntpdc is used with a command line from an untrusted source.
CVE-2018-12327	ntpdate-4.2.6p5-15.el6.centos.x86_64	ntpdate	Stack-based buffer overflow in ntpq and ntpdc of NTP version 4.2.8p11allows an attacker to achieve code execution or escalate to higher privileges via a long string as the argument for an IPv4 or IPv6 command-line parameter. NOTE: It is unclear whether there are any common situations in which ntpq or ntpdc is used with a command line from an untrusted source.

CVE-2018-12384	nss-3.36.0-9.el6_10.x86_64	nss	**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-2018-12384	nss-sysinit-3.36.0-9.el6_10.x86_64	nss-sysinit	**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-2018-12384	nss-tools-3.36.0-9.el6_10.x86_64	nss-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.

Packages updated for Security reasons.

Old Package	New Package	Subsystem
jre1.8-1.8.0_181-fcs.x86_64	jre1.8-1.8.0_191-fcs.x86_64	OS
kernel-2.6.32-754.3.5.el6.x86_64	kernel-2.6.32-754.6.3.el6.x86_64	OS
kernel-firmware-2.6.32-754.3.5.el6.noarch	kernel-firmware-2.6.32-754.6.3.el6.noarch	OS
kernel-headers-2.6.32-754.3.5.el6.x86_64	kernel-headers-2.6.32-754.6.3.el6.x86_64	OS
nspr-4.13.1-1.el6.x86_64	nspr-4.19.0-1.el6.x86_64	Security
nss-3.28.4-4.el6_9.x86_64	nss-3.36.0-9.el6_10.x86_64	Security
nss-sysinit-3.28.4-4.el6_9.x86_64	nss-sysinit-3.36.0-9.el6_10.x86_64	Security
nss-tools-3.28.4-4.el6_9.x86_64	nss-tools-3.36.0-9.el6_10.x86_64	Security
nss-util-3.28.4-1.el6_9.x86_64	nss-util-3.36.0-1.el6.x86_64	Security
ntp-4.2.6p5-12.el6.centos.1.x86_64	ntp-4.2.6p5-15.el6.centos.x86_64	OS
ntpdate-4.2.6p5-12.el6.centos.1.x86_64	ntpdate-4.2.6p5-15.el6.centos.x86_64	OS
perf-2.6.32-754.3.5.el6.x86_64	perf-2.6.32-754.6.3.el6.x86_64	OS

Packages updated not for Security.

Old Package	New Package NOT for CVE	Subsystem
esi-release-3.3.2.0-12332.15.x86_64	esi-release-3.3.2.2-13190.273.x86_64	App
logbase-ui-3.3.2.0-8462.x86_64	logbase-ui-3.3.2.2-8462.x86_64	GUI
lumeta-api-3.3.2.0-12332.x86_64	lumeta-api-3.3.2.2-13174.x86_64	API
lumeta-api-client-3.3.2.0-12304.x86_64	lumeta-api-client-3.3.2.2-12304.x86_64	API
lumeta-console-3.3.2.0-12302.x86_64	lumeta-console-3.3.2.2-12838.x86_64	CLI-ConsoleApp
lumeta-diagnostics-3.3.2.0-12242.x86_64	lumeta-diagnostics-3.3.2.1-12429.x86_64	Debug
lumeta-discovery-agent-3.3.2.0-12232.x86_64	lumeta-discovery-agent-3.3.2.2-13059.x86_64	Collecting/Scanning
lumeta-dxl-3.3.2.0-12306.x86_64	lumeta-dxl-3.3.2.2-12306.x86_64	API
lumeta-install-3.3.2.0-12308.x86_64	lumeta-install-3.3.2.2-13138.x86_64	GUI
lumeta-ireg-3.3.2.0-6550.x86_64	lumeta-ireg-3.3.2.2-6550.x86_64	GUI
lumeta-lib-3.3.2.0-12249.x86_64	lumeta-lib-3.3.2.2-12821.x86_64	GUI
lumeta-pam-3.3.2.0-12308.x86_64	lumeta-pam-3.3.2.1-12406.x86_64	Security
lumeta-ui-3.3.2.0-12230.x86_64	lumeta-ui-3.3.2.2-12991.x86_64	GUI
lumeta-webapp-3.3.2.0-12060.x86_64	lumeta-webapp-3.3.2.2-12060.x86_64	GUI
netflow-capture-1.3.6p1-1.x86_64	netflow-capture-1.3.6p1-2.x86_64	Collecting/Scanning

x15-backend-3.3.2.0-10885.x86_64	x15-backend-3.3.2.2-10885.x86_64	Analytics/BigData

Packages removed.

Packages removed	Subsystem
cryptsetup-luks-1.2.0-11.el6.x86_64	OS
cryptsetup-luks-libs-1.2.0-11.el6.x86_64	OS