USN-4907-1: Linux kernel vulnerabilities

Wen Xu discovered that the xfs file system implementation in the Linux
kernel did not properly validate the number of extents in an inode. An
attacker could use this to construct a malicious xfs image that, when
mounted, could cause a denial of service (system crash).
(CVE-2018-13095)
It was discovered that the priority inheritance futex implementation in the
Linux kernel contained a race condition, leading to a use-after-free
vulnerability. A local attacker could use this to cause a denial of service
(system crash) or possibly execute arbitrary code.
(CVE-2021-3347)

It was discovered that the network block device (nbd) driver in the Linux
kernel contained a use-after-free vulnerability during device setup. A
local attacker with access to the nbd device could use this to cause a
denial of service (system crash) or possibly execute arbitrary code.
(CVE-2021-3348)

USN-4899-2: SpamAssassin vulnerability

USN-4899-1 fixed a vulnerability in SpamAssassin. This update provides
the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:

Damian Lukowski discovered that SpamAssassin incorrectly handled certain CF
files. If a user or automated system were tricked into using a specially-
crafted CF file, a remote attacker could possibly run arbitrary code.

[CentOS-announce] CESA-2021:1072 Important CentOS 7 libldb Security Update

CentOS Errata and Security Advisory 2021:1072 Important
Upstream details at : https://access.redhat.com/errata/RHSA-2021:1072

The following updated files have been uploaded and are currently

syncing to the mirrors: (sha256sum Filename)

x86_64:

67364ca692de365478eee5a94879717c1fae2b7a4ba46d128ec04f0477c8c2b5 ldb-tools-1.5.4-2.el7.x86_64.rpm

36ad5a43df60889dd9c1134cb0e042317befa64f7293f44bc91271fddbbfc7e6 libldb-1.5.4-2.el7.i686.rpm

cec370a7441899c3ffcd47f783a0437d9d649fd4a1252c6c317561f431e537c4 libldb-1.5.4-2.el7.x86_64.rpm

359852ce38e0555b23e78c945070ef67c0599138eac0c52de77a819e8fdebce9 libldb-devel-1.5.4-2.el7.i686.rpm

4d0e360eff9294623b345353bcf2cb4623c50a3e2bf31ace6ba05141150d85fd libldb-devel-1.5.4-2.el7.x86_64.rpm

29124a79cce7024da4f024131a66f80d78a70d73c5fafe6456617633e5b83560 pyldb-1.5.4-2.el7.i686.rpm

8043266fac97f3c92dfeaa8fad590469ad37ab990d86e9ece87829bdd9e0c8ae pyldb-1.5.4-2.el7.x86_64.rpm

b3dbb953a4dc9b8b5ee95024d51d922488db5a0f0ec2ece9bf47d8d5cbbf24fa pyldb-devel-1.5.4-2.el7.i686.rpm

8f596e23215f48c31a9bb115c327431b21431ac93d7279b39dc998ca0bdfc6b8 pyldb-devel-1.5.4-2.el7.x86_64.rpm

Source:

e678f1a0df3c67bd8f6319dbe32013a311d6d797b51284ff7d5e254c2f7a1ff5 libldb-1.5.4-2.el7.src.rpm

_

Johnny Hughes

CentOS Project { http://www.centos.org/ }

irc: hughesjr, #[hidden email]

Twitter: @JohnnyCentOS

_____

CentOS-announce mailing list

[hidden email]

https://lists.centos.org/mailman/listinfo/centos-announce

[CentOS-announce] CESA-2021:1071 Important CentOS 7 kernel Security Update

CentOS Errata and Security Advisory 2021:1071 Important
Upstream details at : https://access.redhat.com/errata/RHSA-2021:1071

The following updated files have been uploaded and are currently

syncing to the mirrors: (sha256sum Filename)

x86_64:

bfe191b783a11c70daf05fb86e81e2e36d80b7dec5eb2243fa223700ce330824 bpftool-3.10.0-1160.24.1.el7.x86_64.rpm

996ee55268c9971d07d38c3217e0fb813a202d1b838963b6db16217069d193db kernel-3.10.0-1160.24.1.el7.x86_64.rpm

33b524d6eec3fc82a17df2220b596193025c1faf20c5939c4271809681f95803 kernel-abi-whitelists-3.10.0-1160.24.1.el7.noarch.rpm

8764032443efee4dc7bfb0ee1a1749205880cd86b230ad538346b697120c5e7 kernel-debug-3.10.0-1160.24.1.el7.x86_64.rpm

e2b80fc90e80e10166a785ab1c718ed12380055d955ab295c5363ad6405fe815 kernel-debug-devel-3.10.0-1160.24.1.el7.x86_64.rpm

52fc84afa30b500c79c2116a67a199c3eba6bbed1b7b171fc4fec483dc2c9f4c kernel-devel-3.10.0-1160.24.1.el7.x86_64.rpm

cda402fcb291052201381d37c733af954d30e2e6e3f24e5b636ae67715e8c0d0 kernel-doc-3.10.0-1160.24.1.el7.noarch.rpm

2a69b561a8c58b7ed126929ce0f305827b54da8604e8f662568fc8ec96090f26 kernel-headers-3.10.0-1160.24.1.el7.x86_64.rpm

150b5e83d6acc1e5a6e22bee18216d6c7e0c581dca489071a61aab70eb9b93fb kernel-tools-3.10.0-1160.24.1.el7.x86_64.rpm

540ad2675ab792c4e347811b9c59c9dfa46be5932ed582b6b0748c7a27660973 kernel-tools-libs-3.10.0-1160.24.1.el7.x86_64.rpm

44904175313b13552ac962d42d456dc5d52bface994ef485f56c33f7f6971440 kernel-tools-libs-devel-3.10.0-1160.24.1.el7.x86_64.rpm

9124221e268619f8424d72980a7b256e0e00ba0639fcf0be1387712d145c7416 perf-3.10.0-1160.24.1.el7.x86_64.rpm

2308127baa502197469a17cef0a36622ccd5c528247af648e424284943e73572 python-perf-3.10.0-1160.24.1.el7.x86_64.rpm

Source:

6fc0eaf2486a736d0793f6165e07c183bb0c8db2c858bd0dbefc1a2b23a052
8b kernel-3.10.0-1160.24.1.el7.src.rpm

_

Johnny Hughes

CentOS Project { http://www.centos.org/ }

irc: hughesjr, #[hidden email]

Twitter: @JohnnyCentOS

_____

CentOS-announce mailing list

[hidden email]

https://lists.centos.org/mailman/listinfo/centos-announce

USN-4896-2: lxml vulnerability

USN-4896-1 fixed a vulnerability in lxml. This update provides the corresponding update for Ubuntu 14.04 ESM.
Original advisory details:

It was discovered that lxml incorrectly handled certain HTML attributes. A
remote attacker could possibly use this issue to perform cross-site
scripting (XSS) attacks.