USN-4729-1: Open vSwitch vulnerability

Joakim Hindersson discovered that Open vSwitch incorrectly parsed certain
network packets. A remote attacker could use this issue to cause a denial
of service, or possibly alter packet classification.

[CentOS-announce] CEBA-2021:0439 CentOS 7 glibc BugFix Update

CentOS Errata and Bugfix Advisory 2021:0439
Upstream details at : https://access.redhat.com/errata/RHBA-2021:0439

The following updated files have been uploaded and are currently

syncing to the mirrors: (sha256sum Filename)

x86_64:

ee561a3f0dd8945edec3478e8426cc324bdf6fc5fe6a31d762cfae60d3e14830 glibc-2.17-323.el7_9.i686.rpm

b2b420ac2c03b3a2e4cadd073857498446180ec51a863fe30335c9da3a963fde glibc-2.17-323.el7_9.x86_64.rpm

f48d75115ac638576d608849a173ace6a70c2430a2e0226487652befdf004b

```
27  glibc-common-2.17-323.el7_9.x86_64.rpm

acbb0c34227bd9c7bba35cfa08b4942dd141ee4ccadd128d8acedaef5e3152
2c  glibc-devel-2.17-323.el7_9.i686.rpm

aab72ef4b89bc4481b87f7aaf225cbdefb62073dddddc7fc7c2b94ab11a0a9
36  glibc-devel-2.17-323.el7_9.x86_64.rpm

9ba71fe357dd09d1913b30b0bd83507588d8cb06eda6f2c15326f3f1384c61
80  glibc-headers-2.17-323.el7_9.x86_64.rpm

eae7a2d2bc9f6058c113c27e6bdea6677a865df0f7924ed51165a2653c2d21
75  glibc-static-2.17-323.el7_9.i686.rpm

49e01e923bc5d1026751341c9a01ab8ef4d50d8b17e94f179de33afcbfb0b2
34  glibc-static-2.17-323.el7_9.x86_64.rpm

cafdbebcda7664e47d81f647d715249983cbe0bb4b063c1d56ab327a8766e2
d0  glibc-utils-2.17-323.el7_9.x86_64.rpm

27d1ba676d3d4007102e714f71f0f4e97d46890c6eed54e5f10720ff65e7ce
a8  nscd-2.17-323.el7_9.x86_64.rpm

Source:

cb68b648ffec5a38b0cef7e6a88fb2dfb6357c8f0a17cf0331376a3cdfd41d
97  glibc-2.17-323.el7_9.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-2021:0411 Important CentOS 7 flatpak Security Update

CentOS Errata and Security Advisory 2021:0411 Important
Upstream details at : https://access.redhat.com/errata/RHSA-2021:0411

The following updated files have been uploaded and are currently

syncing to the mirrors: (sha256sum Filename)

x86_64:

0e230546571aa26c06f1097967584ab4b9e777e7ca6c94d45f8706a36bdccc22 flatpak-1.0.9-10.el7_9.x86_64.rpm

724795eec6065da1df593d22a6a359fc5b241aec5a3916cbec646ff78f2196ba flatpak-builder-1.0.0-10.el7_9.x86_64.rpm

85ac0468355fd6847c79849e947fd3b5d88f606ad3aa6fd06cb4aca3fe3c9f

c8 flatpak-devel-1.0.9-10.el7_9.x86_64.rpm

6a5560cf575ee9bfa9cac85044e94e3bce3ea85e26431c99e41877289cf82b64 flatpak-libs-1.0.9-10.el7_9.x86_64.rpm

Source:

170d39f61f08b19f0c202440b9ac801e8d5e80ec0240b8cd0f3a9d85a3c109d4 flatpak-1.0.9-10.el7_9.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-4717-2: Firefox regression

USN-4717-1 fixed vulnerabilities in Firefox. The update caused a

startup hang in some circumstances. This update fixes the problem.
We apologize for the inconvenience.

Original advisory details:

Multiple security issues were discovered in Firefox. If a user were
tricked in to opening a specially crafted website, an attacker could
potentially exploit these to cause a denial of service, obtain sensitive
information, conduct clickjacking attacks, or execute arbitrary code.

USN-4713-2: Linux kernel vulnerability

It was discovered that the LIO SCSI target implementation in the Linux
kernel performed insufficient identifier checking in certain XCOPY
requests. An attacker with access to at least one LUN in a multiple
backstore environment could use this to expose sensitive information or
modify data.