



CVE-2016-4037

Published on: 05/23/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:20:00 PM UTC

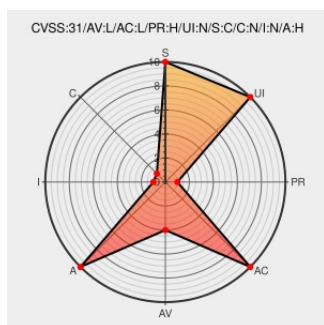
CVE-2016-4037

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The ehci_advance_state function in hw/usb/hcd-ehci.c in QEMU allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) via a circular split isochronous transfer descriptor (siTD) list, a related issue to CVE-2015-8558.

CVE-2016-4037 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	NONE	NONE	HIGH

CVSS2 Score: **4.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
[Qemu-devel] [PATCH 1/2] ehci: apply limit to itd/sidt descriptors	Mailing List Patch Vendor Advisory lists.gnu.org text/x-diff	MLIST [qemu-devel] 20160418 [PATCH 1/2] ehci: apply limit to itd/sidt descriptors

git.qemu.org Git - qemu.git/commit	Patch Vendor Advisory git.qemu.org text/xml	 MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=1ae3f2f178087711f9591350abad133525ba93f2
[SECURITY] [DLA 1599-1] qemu security update	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20181130 [SECURITY] [DLA 1599-1] qemu security update
[SECURITY] Fedora 24 Update: xen-4.6.1-6.fc24	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-48e72b7bc5
[SECURITY] Fedora 23 Update: xen-4.5.3-2.fc23	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-35d7b09908
Re: [Qemu-devel] [PATCH 1/2] ehci: apply limit to itd/sidt descriptors	Mailing List Vendor Advisory lists.gnu.org text/html	 MLIST [qemu-devel] 20160418 Re: [PATCH 1/2] ehci: apply limit to itd/sidt descriptors
oss-security - Re: Qemu: usb: Infinite loop vulnerability in usb_ehci using siTD process	Mailing List www.openwall.com text/html	 MLIST [oss-security] 20160418 Re: Qemu: usb: Infinite loop vulnerability in usb_ehci using siTD process
oss-security - Qemu: usb: Infinite loop vulnerability in usb_ehci using siTD process	Mailing List www.openwall.com text/html	 MLIST [oss-security] 20160418 Qemu: usb: Infinite loop vulnerability in usb_ehci using siTD process
QEMU CVE-2016-4037 Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 86283
USN-2974-1: QEMU vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-2974-1
[SECURITY] Fedora 22 Update: xen-4.5.3-2.fc22	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-75063477ca

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All

Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Application	Qemu	Qemu	2.6.0	rc0	All	All
Application	Qemu	Qemu	2.6.0	rc1	All	All
Application	Qemu	Qemu	2.6.0	rc2	All	All
Application	Qemu	Qemu	2.6.0	rc0	All	All
Application	Qemu	Qemu	2.6.0	rc1	All	All
Application	Qemu	Qemu	2.6.0	rc2	All	All
Application	Qemu	Qemu	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:15.10:***:***:***:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:						

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:*:*:*:
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:22:*:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:
cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:*:
cpe:2.3:a:qemu:qemu:2.6.0:rc0:*:*:*:*:*:*:
cpe:2.3:a:qemu:qemu:2.6.0:rc1:*:*:*:*:*:*:
cpe:2.3:a:qemu:qemu:2.6.0:rc2:*:*:*:*:*:*:
cpe:2.3:a:qemu:qemu:2.6.0:rc0:*:*:*:*:*:*:
cpe:2.3:a:qemu:qemu:2.6.0:rc1:*:*:*:*:*:*:
cpe:2.3:a:qemu:qemu:2.6.0:rc2:*:*:*:*:*:*:
cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE