



CVE-2015-8558

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

Last Modified on: 02/12/2023 11:15:00 PM UTC

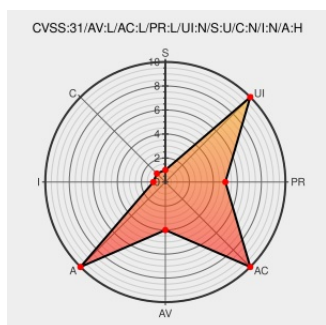
CVE-2015-8558

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The ehci_process_itd 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 isochronous transfer descriptor (iTD) list.

CVE-2015-8558 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	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
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=156a2e4dbffa85997636a7a39ef12da6f1b40254

Debian -- Security Information -- DSA-3471-1 qemu	Third Party Advisory www.debian.org Depreciated Link text/html	 DEBIAN DSA-3471
oss-security - Re: CVE request Qemu: usb: infinite loop in ehci_advance_state results in DoS	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20151214 Re: CVE request Qemu: usb: infinite loop in ehci_advance_state results in DoS
Bug 1277983 – CVE-2015-8558 Qemu: usb: infinite loop in ehci_advance_state results in DoS	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1277983
Debian -- Security Information -- DSA-3469-1 qemu	Third Party Advisory www.debian.org Depreciated Link text/html	 DEBIAN DSA-3469
Debian -- Security Information -- DSA-3470-1 qemu-kvm	Third Party Advisory www.debian.org Depreciated Link text/html	 DEBIAN DSA-3470
QEMU CVE-2015-8558 Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 80694
[Qemu-devel] [PATCH] ehci: make idt processing more robust	Mailing List Patch Third Party Advisory lists.gnu.org text/x-diff	 MLIST [qemu-devel] 20151214 [PATCH] ehci: make idt processing more robust
oss-security - CVE request Qemu: usb: infinite loop in ehci_advance_state results in DoS	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20151214 CVE request Qemu: usb: infinite loop in ehci_advance_state results in DoS
QEMU: Multiple vulnerabilities (GLSA 201602-01) — Gentoo security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201602-01

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	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating Svstem	Debian	Debian Linux	7.0	All	All	All

System						
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All
cpe:2.3:o:debian:debian_linux:7.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:o:debian:debian_linux:7.0:*****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:						
cpe:2.3:a:qemu:qemu:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)