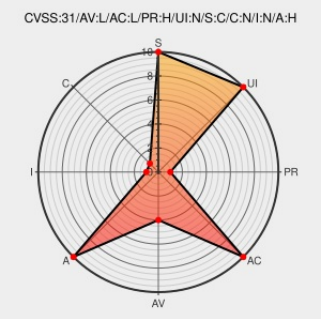
CVE-2016-8667

Published on: 11/04/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:06:58 PM UTC

CVE-2016-8667

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

The rc4030_write function in hw/dma/rc4030.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (divide-by-zero error and QEMU process crash) via a large interval timer reload value.

CVE-2016-8667 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: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 1497-1] qemu security update	Mailing List, Third Party Advisory, lists.debian.org, text/html	MLIST [debian-lts-announce] 20180906 [SECURITY] [DLA 1497-1] qemu security update

oss-security - CVE request Qemu: dma: rc4030 divide by zero error in set_next_tick	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20161014 CVE request Qemu: dma: rc4030 divide by zero error in set_next_tick
openSUSE-SU-2016:3237-1: moderate: Security update for qemu	Mailing List Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2016:3237
QEMU 'hw/dma/rc4030.c' Divide By Zero Denial of Service Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 93567
oss-security - Re: CVE request Qemu: dma: rc4030 divide by zero error in set_next_tick	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20161015 Re: CVE request Qemu: dma: rc4030 divide by zero error in set_next_tick
[Qemu-devel] [PATCH] dma: rc4030: limit interval timer reload value	Patch Third Party Advisory lists.gnu.org text/x-diff	MLIST [qemu-devel] 20161012 [PATCH] dma: rc4030: limit interval timer reload value

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	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Application	Qemu	Qemu	2.9.0	rc0	All	All
Application	Qemu	Qemu	2.9.0	rc0	All	All
Application	Qemu	Qemu	All	All	All	All

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.2:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:42.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.9.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.9.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→