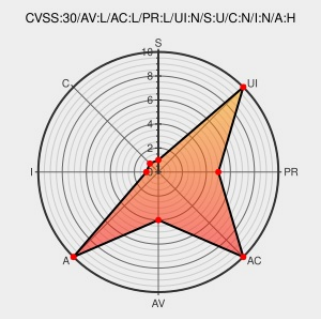
CVE-2015-8817

Published on: 12/29/2016 12:00:00 AM UTC

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

CVE-2015-8817

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



Certain versions of Qemu from Qemu contain the following vulnerability:

QEMU (aka Quick Emulator) built to use 'address_space_translate' to map an address to a MemoryRegionSection is vulnerable to an OOB r/w access issue. It could occur while doing pci_dma_read/write calls. Affects QEMU versions >= 1.6.0 and <= 2.3.1. A privileged user inside guest could use this flaw to crash the guest instance resulting in DoS.

CVE-2015-8817 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: 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
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:2705
Red Hat Customer Portal	access.redhat.com	MISC access.redhat.com/errata/RHSA-2016:2671

	text/html	
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2704
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:2670
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:2704
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2670
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2706
CVE-2015-8817 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2015-8817
oss-security - CVE request Qemu: OOB access in address_space_rw leads to segmentation fault	Mailing List Patch www.openwall.com text/html	MLIST [oss-security] 20160301 CVE request Qemu: OOB access in address_space_rw leads to segmentation fault
git.qemu.org Git - qemu.git/commit	Issue Tracking web.archive.org text/xml Inactive Link Not Archived	MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=23820dbfc79d1c9dce090b4c555994f2bb6a69b3
oss-security - Re: CVE request Qemu: OOB access in address_space_rw leads to segmentation fault	Mailing List Patch www.openwall.com text/html	MLIST [oss-security] 20160301 Re: CVE request Qemu: OOB access in address_space_rw leads to segmentation fault
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2016:2706
git.qemu.org Git - qemu.git/commit	Issue Tracking web.archive.org text/xml Inactive Link Not Archived	MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=c3c1bb99d1c11978d9ce94d1bdcf0705378c1459
Bug 1300771 – CVE-2015-8817 CVE-2015-8818 Qemu: OOB access in address_space_rw leads to segmentation fault	Issue Tracking bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1300771
[Qemu-stable] [PATCH for v2.3.1] exec: Respect as_translate_internal len	Mailing List lists.gnu.org text/x-diff	MLIST [qemu-stable] 20160127 [PATCH for v2.3.1] exec: Respect as_translate_internal length clamp
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2705
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:2671

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
Application	Qemu	Qemu	1.6.0	All	All	All
Application	Qemu	Qemu	1.6.0	rc1	All	All
Application	Qemu	Qemu	1.6.0	rc2	All	All
Application	Qemu	Qemu	1.6.0	rc3	All	All
Application	Qemu	Qemu	1.6.1	All	All	All
Application	Qemu	Qemu	1.6.2	All	All	All
Application	Qemu	Qemu	1.7.1	All	All	All
Application	Qemu	Qemu	2.0.0	-	All	All
Application	Qemu	Qemu	2.0.0	rc0	All	All
Application	Qemu	Qemu	2.0.0	rc1	All	All
Application	Qemu	Qemu	2.0.0	rc2	All	All
Application	Qemu	Qemu	2.0.0	rc3	All	All
Application	Qemu	Qemu	2.0.2	All	All	All
Application	Qemu	Qemu	2.1.0	All	All	All
Application	Qemu	Qemu	2.1.0	rc0	All	All
Application	Qemu	Qemu	2.1.0	rc1	All	All
Application	Qemu	Qemu	2.1.0	rc2	All	All
Application	Qemu	Qemu	2.1.0	rc3	All	All
Application	Qemu	Qemu	2.1.0	rc5	All	All
Application	Qemu	Qemu	2.1.1	All	All	All
Application	Qemu	Qemu	2.1.2	All	All	All
Application	Qemu	Qemu	2.1.3	All	All	All
Application	Qemu	Qemu	2.2.0	All	All	All
Application	Qemu	Qemu	2.2.1	All	All	All
Application	Qemu	Qemu	2.3.0	All	All	All
Application	Qemu	Qemu	2.3.1	All	All	All
Application	Qemu	Qemu	1.6.0	All	All	All
Application	Qemu	Qemu	1.6.0	rc1	All	All
Application	Qemu	Qemu	1.6.0	rc2	All	All

Application	Qemu	Qemu	1.6.0	rc3	All	All
Application	Qemu	Qemu	1.6.1	All	All	All
Application	Qemu	Qemu	1.6.2	All	All	All
Application	Qemu	Qemu	1.7.1	All	All	All
Application	Qemu	Qemu	2.0.0	-	All	All
Application	Qemu	Qemu	2.0.0	rc0	All	All
Application	Qemu	Qemu	2.0.0	rc1	All	All
Application	Qemu	Qemu	2.0.0	rc2	All	All
Application	Qemu	Qemu	2.0.0	rc3	All	All
Application	Qemu	Qemu	2.0.2	All	All	All
Application	Qemu	Qemu	2.1.0	All	All	All
Application	Qemu	Qemu	2.1.0	rc0	All	All
Application	Qemu	Qemu	2.1.0	rc1	All	All
Application	Qemu	Qemu	2.1.0	rc2	All	All
Application	Qemu	Qemu	2.1.0	rc3	All	All
Application	Qemu	Qemu	2.1.0	rc5	All	All
Application	Qemu	Qemu	2.1.1	All	All	All
Application	Qemu	Qemu	2.1.2	All	All	All
Application	Qemu	Qemu	2.1.3	All	All	All
Application	Qemu	Qemu	2.2.0	All	All	All
Application	Qemu	Qemu	2.2.1	All	All	All
Application	Qemu	Qemu	2.3.0	All	All	All
Application	Qemu	Qemu	2.3.1	All	All	All

cpe:2.3:a:qemu:qemu:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:-:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc5:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.6.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.7.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:-:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.0:rc5:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:2.3.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→