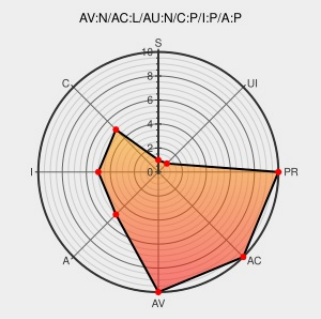
CVE-2013-4150

Published on: 11/04/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:44:00 AM UTC

CVE-2013-4150

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



Certain versions of Qemu from Qemu contain the following vulnerability:

The virtio_net_load function in hw/net/virtio-net.c in QEMU 1.5.0 through 1.7.x before 1.7.2 allows remote attackers to cause a denial of service or possibly execute arbitrary code via vectors in which the value of curr_queues is greater than max_queues, which triggers an out-of-bounds write.

CVE-2013-4150 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
[Qemu-stable] [ANNOUNCE] QEMU 1.7.2 Stable released	Patch, lists.nongnu.org, text/html	MLIST [Qemu-stable] 20140723 [ANNOUNCE] QEMU 1.7.2 Stable released
git.qemu.org Git - qemu.git/commit	web.archive.org, text/xml, Inactive Link, Not Archived	MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=eea750a5623ddac7a61982eec8f1c93481857578
Red Hat Customer Portal	access.redhat.com, text/html	MISC access.redhat.com/errata/RHSA-2014:0927
Red Hat Customer Portal	Patch, Vendor Advisory, web.archive.org, text/html	REDHAT RHSA-2014:0927

	Inactive Link Not Archived	
[SECURITY] Fedora 20 Update: qemu-1.6.2-5.fc20	lists.fedoraproject.org text/html	FEDORA FEDORA-2014-6288
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:1268
CVE-2013-4150 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2013-4150
Bug 1066340 – CVE-2013-4150 qemu: virtio-net: out-of-bounds buffer write on invalid state load	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1066340

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	1.5.0	All	All	All
Application	Qemu	Qemu	1.5.0	rc1	All	All
Application	Qemu	Qemu	1.5.0	rc2	All	All
Application	Qemu	Qemu	1.5.0	rc3	All	All
Application	Qemu	Qemu	1.5.1	All	All	All
Application	Qemu	Qemu	1.5.2	All	All	All
Application	Qemu	Qemu	1.5.3	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	1.5.0	All	All	All
Application	Qemu	Qemu	1.5.0	rc1	All	All
Application	Qemu	Qemu	1.5.0	rc2	All	All
Application	Qemu	Qemu	1.5.0	rc3	All	All
Application	Qemu	Qemu	1.5.1	All	All	All

Application	Qemu	Qemu	1.5.2	All	All	All
Application	Qemu	Qemu	1.5.3	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

cpe:2.3:a:qemu:qemu:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.3:*:*:*:*:*:*:*:

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:1.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.5.3:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→