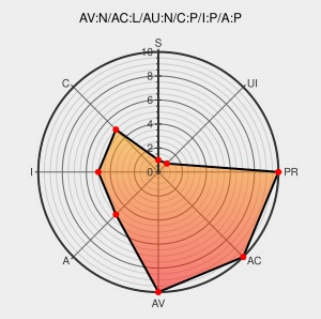
CVE-2013-4148

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

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

CVE-2013-4148

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



Certain versions of Qemu from Qemu contain the following vulnerability:

Integer signedness error in the virtio_net_load function in hw/net/virtio-net.c in QEMU 1.x before 1.7.2 allows remote attackers to execute arbitrary code via a crafted savevm image, which triggers a buffer overflow.

CVE-2013-4148 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
access.redhat.com | CVE-2013-4148	access.redhat.com, text/html	MISC access.redhat.com/security/cve/CVE-2013-4148
git.qemu.org Git - qemu.git/commitdiff	web.archive.org, text/xml, Inactive Link, Not Archived	MISC git.qemu.org/?p=qemu.git%3Ba=commitdiff%3Bh=71f7fe48e10a8437c9d42d859389f37157f59980
Red Hat Customer Portal	Patch, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2014:0744

Red Hat Customer Portal	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:0743
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:0927
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:0674
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:0743
[SECURITY] Fedora 20 Update: qemu-1.6.2-5.fc20	lists.fedoraproject.org text/html	FEDORA FEDORA-2014-6288
Bug 1066334 – CVE-2013-4148 qemu: virtio-net: buffer overflow on invalid state load	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1066334
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:1268
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:0888
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:0744

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	1.0	All	All	All
Application	Qemu	Qemu	1.0	rc1	All	All
Application	Qemu	Qemu	1.0	rc2	All	All
Application	Qemu	Qemu	1.0	rc3	All	All
Application	Qemu	Qemu	1.0	rc4	All	All
Application	Qemu	Qemu	1.0.1	All	All	All
Application	Qemu	Qemu	1.1	All	All	All
Application	Qemu	Qemu	1.1	rc1	All	All
Application	Qemu	Qemu	1.1	rc2	All	All
Application	Qemu	Qemu	1.1	rc3	All	All
Application	Qemu	Qemu	1.1	rc4	All	All

Application	Qemu	Qemu	1.4.1	All	All	All
Application	Qemu	Qemu	1.4.2	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
Application	Qemu	Qemu	1.0	All	All	All
Application	Qemu	Qemu	1.0	rc1	All	All
Application	Qemu	Qemu	1.0	rc2	All	All
Application	Qemu	Qemu	1.0	rc3	All	All
Application	Qemu	Qemu	1.0	rc4	All	All
Application	Qemu	Qemu	1.0.1	All	All	All
Application	Qemu	Qemu	1.1	All	All	All
Application	Qemu	Qemu	1.1	rc1	All	All
Application	Qemu	Qemu	1.1	rc2	All	All
Application	Qemu	Qemu	1.1	rc3	All	All
Application	Qemu	Qemu	1.1	rc4	All	All
Application	Qemu	Qemu	1.4.1	All	All	All
Application	Qemu	Qemu	1.4.2	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:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0:rc4:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:rc4:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.4.2:*:*:*:*:*:*:*:

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:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0:rc4:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:rc3:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.1:rc4:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:qemu:qemu:1.4.2:*:*:*:*:*:*:*:

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→