



CVE-2013-4149

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

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

CVE-2013-4149

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Buffer overflow in virtio_net_load function in net/virtio-net.c in QEMU 1.3.0 through 1.7.x before 1.7.2 might allow remote attackers to execute arbitrary code via a large MAC table.

CVE-2013-4149 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=98f93ddd84800f207889491e0b5d851386b459cf](#)

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](#)
[Inactive Link](#) [Not Archived](#)

[REDHAT RHSA-2014:0927](#)

[SECURITY] Fedora 20 Update: qemu-1.6.2-5.fc20	lists.fedoraproject.org text/html	 FEDORA FEDORA-2014-6288
access.redhat.com CVE-2013-4149	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2013-4149
Red Hat Customer Portal	access.redhat.com text/html	 MISC access.redhat.com/errata/RHSA-2014:1268
Bug 1066337 – CVE-2013-4149 qemu: virtio-net: out-of-bounds buffer write on load	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=1066337

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
Application	Qemu	Qemu	1.3.0	All	All	All
Application	Qemu	Qemu	1.3.0	rc0	All	All
Application	Qemu	Qemu	1.3.0	rc1	All	All
Application	Qemu	Qemu	1.3.0	rc2	All	All
Application	Qemu	Qemu	1.3.1	All	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	1.7.1	All	All	All
Application	Qemu	Qemu	1.3.0	All	All	All
Application	Qemu	Qemu	1.3.0	rc0	All	All
Application	Qemu	Qemu	1.3.0	rc1	All	All
Application	Qemu	Qemu	1.3.0	rc2	All	All
Application	Qemu	Qemu	1.3.1	All	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:1.3.0:*****:						
cpe:2.3:a:qemu:qemu:1.3.0:rc0:*****:						
cpe:2.3:a:qemu:qemu:1.3.0:rc1:*****:						
cpe:2.3:a:qemu:qemu:1.3.0:rc2:*****:						
cpe:2.3:a:qemu:qemu:1.3.1:*****:						
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:1.3.0:*****:
cpe:2.3:a:qemu:qemu:1.3.0:rc0:*****:
cpe:2.3:a:qemu:qemu:1.3.0:rc1:*****:
cpe:2.3:a:qemu:qemu:1.3.0:rc2:*****:
cpe:2.3:a:qemu:qemu:1.3.1:*****:
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:1.6.1:*****:
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→