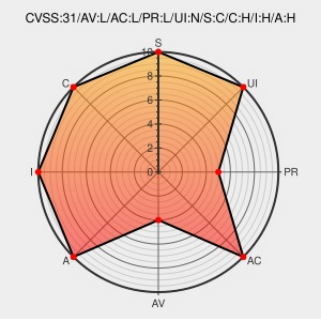
CVE-2013-4535

Published on: 02/11/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:27 PM UTC

CVE-2013-4535

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



Certain versions of Qemu from Qemu contain the following vulnerability:

The virtqueue_map_sg function in hw/virtio/virtio.c in QEMU before 1.7.2 allows remote attackers to execute arbitrary files via a crafted savevm image, related to virtio-block or virtio-serial read.

CVE-2013-4535 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC rhn.redhat.com/errata/RHSA-2014-0743.html

Bug 1066401 – CVE-2013-4535 CVE-2013-4536 qemu: virtio: insufficient validation of num_sg when mapping	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1066401
[Qemu-stable] [ANNOUNCE] QEMU 1.7.2 Stable released	Third Party Advisory lists.nongnu.org text/html	MISC lists.nongnu.org/archive/html/qemu-stable/2014-07/msg00187.html
[SECURITY] Fedora 20 Update: qemu-1.6.2-5.fc20	Third Party Advisory lists.fedoraproject.org text/html	MISC lists.fedoraproject.org/pipermail/package-announce/2014-May/133345.html
git.qemu.org Git - qemu.git/commitdiff	Patch Vendor Advisory git.qemu.org text/xml	MISC git.qemu.org/?p=qemu.git;a=commitdiff;h=36cf2a37132c7f01fa9adb5f95f5312b27742fd4
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC rhn.redhat.com/errata/RHSA-2014-0744.html

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	All	All	All	All
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All
Application	Redhat	Virtualization	3.0	All	All	All

Application	Redhat	Virtualization	3.0	All	All	All

cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:
cpe:2.3:a:qemu:qemu:*:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_tus:6.5:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_tus:6.5:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:
cpe:2.3:a:redhat:virtualization:3.0:*:*:*:*:*:*:*:
cpe:2.3:a:redhat:virtualization:3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→