



CVE-2014-0148

Published on: 02/10/2020 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:33:00 AM UTC

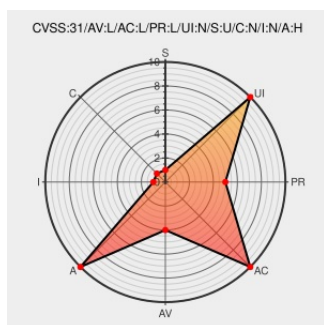
CVE-2014-0148

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Qemu before 2.0 block driver for Hyper-V VHDX Images is vulnerable to infinite loops and other potential issues when calculating BAT entries, due to missing bounds checks for block_size and logical_sector_size variables. These are used to derive other fields like 'sectors_per_block' etc. A user able to alter the Qemu disk image could use this flaw to crash the Qemu instance resulting in DoS.

CVE-2014-0148 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

CVE References

Description	Tags	Link
Red Hat Customer Portal	rhn.redhat.com text/html	MISC rhn.redhat.com/errata/RHSA-2014-0421.html
Red Hat Customer Portal	rhn.redhat.com text/html	MISC rhn.redhat.com/errata/RHSA-2014-0420.html
git.qemu.org Git - qemu.git/commit	git.qemu.org text/xml	MISC git.qemu.org/?p=qemu.git;a=commit;h=1d7678dec4761acdc43439da6ceda41a703ba1a6
oss-security - QEMU image format input validation fixes (multiple CVEs)	www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2014/03/26/8
cve-website	www.cve.org text/html	MISC www.cve.org/CVERecord?id=CVE-2014-0148

[Qemu-devel] [PATCH for-2.0 00/47]
block: image format input validation

[lists.gnu.org](https://lists.gnu.org/archive/html/qemu-devel/2014-03/msg04994.html)
text/html

 [MISC lists.gnu.org/archive/html/qemu-devel/2014-03/msg04994.html](https://lists.gnu.org/archive/html/qemu-devel/2014-03/msg04994.html)

1078212 – (CVE-2014-0148) CVE-2014-0148 Qemu: vhd: bounds checking for block_size and logical_sector_size

[bugzilla.redhat.com](https://bugzilla.redhat.com/show_bug.cgi?id=1078212)
text/html

 [MISC bugzilla.redhat.com/show_bug.cgi?id=1078212](https://bugzilla.redhat.com/show_bug.cgi?id=1078212)

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	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Openstack Platform	5	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	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
Application	Redhat	Virtualization	3.0	All	All	All

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

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*****:

cpe:2.3:o:redhat:enterprise_linux_eus:6.5:*****:

cpe:2.3:o:redhat:enterprise_linux_openstack_platform:5:*****:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*****:

cpe:2.3:o:redhat:enterprise_linux_server_aus: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:a:redhat:virtualization:3.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)