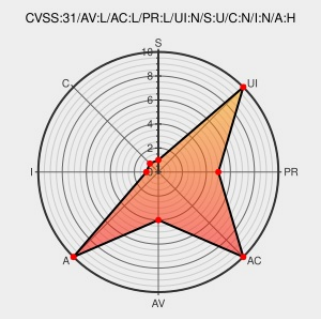
CVE-2014-0148

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 ise 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 text/html	MISC lists.gnu.org/archive/html/qemu-devel/2014-03/msg04994.html
1078212 – (CVE-2014-0148) CVE-2014-0148 Qemu: vhdx: bounds checking for block_size and logical_sector_size	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1078212

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 and Source URL Uptime Status status.cve.report