



CVE-2014-0222

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-0222
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-04 21:55:00 UTC
Updated	2023-02-13 00:37:00 UTC
Description	Integer overflow in the qcow_open function in block/qcow.c in QEMU before 1.7.2 allows remote attackers to cause a denial of service (crash) via a crafted image file.

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	0.1.0	All	All	All
Application	Qemu	Qemu	0.1.1	All	All	All
Application	Qemu	Qemu	0.1.2	All	All	All
Application	Qemu	Qemu	0.1.3	All	All	All
Application	Qemu	Qemu	0.1.4	All	All	All
Application	Qemu	Qemu	0.1.5	All	All	All
Application	Qemu	Qemu	0.1.6	All	All	All
Application	Qemu	Qemu	0.10.0	All	All	All
Application	Qemu	Qemu	0.10.1	All	All	All
Application	Qemu	Qemu	0.10.2	All	All	All
Application	Qemu	Qemu	0.10.3	All	All	All
Application	Qemu	Qemu	0.10.4	All	All	All
Application	Qemu	Qemu	0.10.5	All	All	All
Application	Qemu	Qemu	0.10.6	All	All	All
Application	Qemu	Qemu	0.11.0	All	All	All
Application	Qemu	Qemu	0.11.0	rc0	All	All
Application	Qemu	Qemu	0.11.0	rc1	All	All

Application	Qemu	Qemu	0.11.0	rc2	All	All
Application	Qemu	Qemu	0.11.0-rc0	All	All	All
Application	Qemu	Qemu	0.11.0-rc1	All	All	All
Application	Qemu	Qemu	0.11.0-rc2	All	All	All
Application	Qemu	Qemu	0.11.1	All	All	All
Application	Qemu	Qemu	0.12.0	All	All	All
Application	Qemu	Qemu	0.12.0	rc1	All	All
Application	Qemu	Qemu	0.12.0	rc2	All	All
Application	Qemu	Qemu	0.12.1	All	All	All
Application	Qemu	Qemu	0.12.2	All	All	All
Application	Qemu	Qemu	0.12.3	All	All	All
Application	Qemu	Qemu	0.12.4	All	All	All
Application	Qemu	Qemu	0.12.5	All	All	All
Application	Qemu	Qemu	0.13.0	All	All	All
Application	Qemu	Qemu	0.13.0	rc0	All	All
Application	Qemu	Qemu	0.13.0	rc1	All	All
Application	Qemu	Qemu	0.14.0	All	All	All
Application	Qemu	Qemu	0.14.0	rc0	All	All
Application	Qemu	Qemu	0.14.0	rc1	All	All
Application	Qemu	Qemu	0.14.0	rc2	All	All
Application	Qemu	Qemu	0.14.1	All	All	All
Application	Qemu	Qemu	0.15.0	rc1	All	All
Application	Qemu	Qemu	0.15.0	rc2	All	All
Application	Qemu	Qemu	0.15.1	All	All	All
Application	Qemu	Qemu	0.15.2	All	All	All
Application	Qemu	Qemu	0.2.0	All	All	All
Application	Qemu	Qemu	0.3.0	All	All	All
Application	Qemu	Qemu	0.4.0	All	All	All
Application	Qemu	Qemu	0.4.1	All	All	All
Application	Qemu	Qemu	0.4.2	All	All	All
Application	Qemu	Qemu	0.4.3	All	All	All
Application	Qemu	Qemu	0.5.0	All	All	All
Application	Qemu	Qemu	0.5.1	All	All	All
Application	Qemu	Qemu	0.5.2	All	All	All
Application	Qemu	Qemu	0.5.3	All	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	0.1.0	All	All	All
Application	Qemu	Qemu	0.1.1	All	All	All
Application	Qemu	Qemu	0.1.2	All	All	All
Application	Qemu	Qemu	0.1.3	All	All	All
Application	Qemu	Qemu	0.1.4	All	All	All
Application	Qemu	Qemu	0.1.5	All	All	All
Application	Qemu	Qemu	0.1.6	All	All	All
Application	Qemu	Qemu	0.10.0	All	All	All
Application	Qemu	Qemu	0.10.1	All	All	All
Application	Qemu	Qemu	0.10.2	All	All	All
Application	Qemu	Qemu	0.10.3	All	All	All
Application	Qemu	Qemu	0.10.4	All	All	All
Application	Qemu	Qemu	0.10.5	All	All	All
Application	Qemu	Qemu	0.10.6	All	All	All
Application	Qemu	Qemu	0.11.0	All	All	All
Application	Qemu	Qemu	0.11.0	rc0	All	All
Application	Qemu	Qemu	0.11.0	rc1	All	All
Application	Qemu	Qemu	0.11.0	rc2	All	All
Application	Qemu	Qemu	0.11.0-rc0	All	All	All
Application	Qemu	Qemu	0.11.0-rc1	All	All	All
Application	Qemu	Qemu	0.11.0-rc2	All	All	All
Application	Qemu	Qemu	0.11.1	All	All	All
Application	Qemu	Qemu	0.12.0	All	All	All
Application	Qemu	Qemu	0.12.0	rc1	All	All
Application	Qemu	Qemu	0.12.0	rc2	All	All
Application	Qemu	Qemu	0.12.1	All	All	All
Application	Qemu	Qemu	0.12.2	All	All	All
Application	Qemu	Qemu	0.12.3	All	All	All
Application	Qemu	Qemu	0.12.4	All	All	All
Application	Qemu	Qemu	0.12.5	All	All	All
Application	Qemu	Qemu	0.13.0	All	All	All
Application	Qemu	Qemu	0.13.0	rc0	All	All

Application	Qemu	Qemu	0.13.0	rc1	All	All
Application	Qemu	Qemu	0.14.0	All	All	All
Application	Qemu	Qemu	0.14.0	rc0	All	All
Application	Qemu	Qemu	0.14.0	rc1	All	All
Application	Qemu	Qemu	0.14.0	rc2	All	All
Application	Qemu	Qemu	0.14.1	All	All	All
Application	Qemu	Qemu	0.15.0	rc1	All	All
Application	Qemu	Qemu	0.15.0	rc2	All	All
Application	Qemu	Qemu	0.15.1	All	All	All
Application	Qemu	Qemu	0.15.2	All	All	All
Application	Qemu	Qemu	0.2.0	All	All	All
Application	Qemu	Qemu	0.3.0	All	All	All
Application	Qemu	Qemu	0.4.0	All	All	All
Application	Qemu	Qemu	0.4.1	All	All	All
Application	Qemu	Qemu	0.4.2	All	All	All
Application	Qemu	Qemu	0.4.3	All	All	All
Application	Qemu	Qemu	0.5.0	All	All	All
Application	Qemu	Qemu	0.5.1	All	All	All
Application	Qemu	Qemu	0.5.2	All	All	All
Application	Qemu	Qemu	0.5.3	All	All	All
Application	Qemu	Qemu	0.5.4	All	All	All
Application	Qemu	Qemu	0.5.5	All	All	All
Application	Qemu	Qemu	0.6.0	All	All	All
Application	Qemu	Qemu	0.6.1	All	All	All
Application	Qemu	Qemu	0.7.0	All	All	All
Application	Qemu	Qemu	0.7.1	All	All	All
Application	Qemu	Qemu	0.7.2	All	All	All
Application	Qemu	Qemu	0.8.0	All	All	All
Application	Qemu	Qemu	0.8.1	All	All	All
Application	Qemu	Qemu	0.8.2	All	All	All
Application	Qemu	Qemu	0.9.0	All	All	All
Application	Qemu	Qemu	0.9.1	All	All	All
Application	Qemu	Qemu	0.9.1-5	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	All	All	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp1	All	All
Operating System	Suse	Linux Enterprise Server	11.0	sp1	All	All

References			
Reference	Source	Link	Tag
[SECURITY] Fedora 20 Update: qemu-1.6.2-6.fc20	FEDORA	lists.fedoraproject.org	
[Qemu-stable] [ANNOUNCE] QEMU 1.7.2 Stable released	MLIST	lists.nongnu.org	Patch
Red Hat Customer Portal	MISC	access.redhat.com	
openSUSE-SU-2015:1965-1: moderate: Security update for xen	SUSE	lists.opensuse.org	
Red Hat Customer Portal	MISC	access.redhat.com	
[Qemu-devel] [PATCH 3/5] qcow1: Validate L2 table size (CVE-2014-0222)	MLIST	lists.gnu.org	Exploit

Red Hat Customer Portal	MISC	access.redhat.com	
Red Hat Customer Portal	MISC	access.redhat.com	
Red Hat Customer Portal	MISC	access.redhat.com	
Bug 1097216 – CVE-2014-0222 Qemu: qcow1: validate L2 table size to avoid integer overflows	MISC	bugzilla.redhat.com	
[security-announce] SUSE-SU-2015:0929-1: important: Security update for	SUSE	lists.opensuse.org	
[SECURITY] Fedora 20 Update: qemu-1.6.2-5.fc20	FEDORA	lists.fedoraproject.org	
Red Hat Customer Portal	MISC	access.redhat.com	
access.redhat.com CVE-2014-0222	MISC	access.redhat.com	
Debian -- Security Information -- DSA-3044-1 qemu-kvm	DEBIAN	www.debian.org	
QEMU L2 Table Size Validation Integer Overflow Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report