



CVE-2011-2212

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2011-2212
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-21 15:55:09 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Buffer overflow in the virtio subsystem in qemu-kvm 0.14.0 and earlier allows privileged guest users to cause a denial of service.

Risk And Classification

Primary CVSS: v2.0 7.4 from nvd@nist.gov

AV:A/AC:M/Au:S/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Adjacent

Access Complexity

Medium

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:A/AC:M/Au:S/C:C/I:C/A:C

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	rc0	All	All
Application	Qemu	Qemu	0.14.0	rc1	All	All
Application	Qemu	Qemu	0.14.0	rc2	All	All
Application	Qemu	Qemu	0.2.0	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	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference					Source	
Debian update for qemu-kvm - Secunia.com					af854a3a-2127-422b-91ae-3	
Debian -- Security Information -- DSA-2282-1 qemu-kvm					af854a3a-2127-422b-91ae-3	
Qemu Multiple Vulnerabilities - Secunia.com					af854a3a-2127-422b-91ae-3	
KVM qemu-kvm Multiple Vulnerabilities - Secunia.com					af854a3a-2127-422b-91ae-3	
SUSE update for kvm - Secunia.com					af854a3a-2127-422b-91ae-3	
access.redhat.com					af854a3a-2127-422b-91ae-3	

713589 – (CVE-2011-2212) CVE-2011-2212 qemu-kvm: virtqueue: too-large indirect descriptor buffer overflow	af854a3a-2127-422b-91ae-3
hermes.opensuse.org/messages/9605323	af854a3a-2127-422b-91ae-3
USN-1165-1: QEMU vulnerabilities Ubuntu	af854a3a-2127-422b-91ae-3
Red Hat update for qemu-kvm - Secunia.com	af854a3a-2127-422b-91ae-3
www.osvdb.org/74751	af854a3a-2127-422b-91ae-3
[security-announce] openSUSE-SU-2011:0803-1: important: kvm	af854a3a-2127-422b-91ae-3
Ubuntu update for qemu-kvm - Secunia.com	af854a3a-2127-422b-91ae-3
Red Hat Customer Portal	MITRE
CVE-2011-2212 - Red Hat Customer Portal	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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