



CVE-2015-3456

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

Summary

CVE	CVE-2015-3456
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-13 18:59:00 UTC
Updated	2023-11-07 02:25:00 UTC
Description	The Floppy Disk Controller (FDC) in QEMU, as used in Xen 4.5.x and earlier and KVM, allows local guest users to cause a

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Enterprise Virtualization	3.0	All	All	All
Application	Redhat	Enterprise Virtualization	3.0	All	All	All
Application	Redhat	Openstack	4.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All
Application	Redhat	Openstack	4.0	All	All	All
Application	Redhat	Openstack	5.0	All	All	All
Application	Redhat	Openstack	6.0	All	All	All
Application	Redhat	Openstack	7.0	All	All	All

Operating System	Xen	Xen	4.5.0	All	All	All
Operating System	Xen	Xen	4.5.0	All	All	All

References

Reference

[security-announce] openSUSE-SU-2015:0983-1: important: Security update

CVE-2015-3456

Red Hat Customer Portal

Debian -- Security Information -- DSA-3274-1 virtualbox

[security-announce] SUSE-SU-2015:0923-1: important: Security update for

QEMU 'hw/block/fdc.c' VENOM Remote Memory Corruption Vulnerability

[security-announce] openSUSE-SU-2015:0894-1: important: Security update

Red Hat Customer Portal

McAfee KnowledgeBase - Intel Security - Security Bulletin: Advanced Threat Defense update for Venom vulnerability

VENOM, don't get bitten. | Red Hat Security

Xen Floppy Disk Controller Emulation Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker

Oracle Critical Patch Update - July 2015

2017-04 Security Bulletin: Multiple Vulnerabilities in NorthStar Controller Application before version 2.1.0 Service Pack 1. - Juniper Networks

git.qemu.org Git - qemu.git/commitdiff

Broadcom Support Portal

VENOM: QEMU vulnerability (CVE-2015-3456) - Red Hat Customer Portal

Red Hat Customer Portal

'[security bulletin] HPSBMU03336 rev.1- HP Helion OpenStack affected by VENOM, Denial of Service (DoS' - MARC

[SECURITY] Fedora 21 Update: qemu-2.1.3-7.fc21

VirtualBox: Multiple vulnerabilities (GLSA 201612-27) — Gentoo security

openSUSE-SU-2015:1400-1: moderate: Security update for virtualbox

USN-2608-1: QEMU vulnerabilities | Ubuntu

Oracle PeopleSoft Products Lets Local Users Gain Elevated Privileges and Remote Users Partially Access Data and Partially Deny Service - S

QEMU Floppy Disk Controller Emulation Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker

git.qemu.org Git - qemu.git/commitdiff

Red Hat Customer Portal

Arista - Security Advisory 0010

[security-announce] SUSE-SU-2015:0927-1: important: Security update for

VENOM Vulnerability

FortiGuard

[security-announce] SUSE-SU-2015:0929-1: important: Security update for

Red Hat Customer Portal

Venom - Lenovo Support (US)

Debian -- Security Information -- DSA-3262-1 xen

Red Hat Customer Portal

Red Hat Customer Portal

[security-announce] openSUSE-SU-2015:0893-1: important: Security update

Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security

Object not found!

Red Hat Customer Portal

'[security bulletin] HPSBMU03349 rev.1- HP Helion CloudSystem, Local Denial of Service (DoS), Arbitra' - MARC

XSA-133 - Xen Security Advisories

Debian -- Security Information -- DSA-3259-1 qemu

Citrix Security Advisory for CVE-2015-3456

Security Advisory - VENOM Vulnerability in Huawei Products - Huawei PSIRT

[security-announce] SUSE-SU-2015:0889-1: important: Security update for

2015-07 Security Bulletin: Buffer overflow vulnerability in QEMU component of the KVM/QEMU and Xen hypervisors (CVE-2015-3456) aka VE

QEMU: Multiple vulnerabilities (GLSA 201602-01) — Gentoo security

QEMU - Floppy Disk Controller (FDC) (PoC)

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

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

© 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 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