



CVE-2015-5154

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

Summary

CVE	CVE-2015-5154
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-12 14:59:00 UTC
Updated	2023-02-13 00:50:00 UTC
Description	Heap-based buffer overflow in the IDE subsystem in QEMU, as used in Xen 4.5.x and earlier, when the container has a CD

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	22	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp4	All	All
Application	Suse	Linux Enterprise Debuginfo	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Server	11	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All

Operating System	Suse	Linux Enterprise Software Development Kit	11	sp4	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All
Operating System	Suse	Suse Linux Enterprise Server	12	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	4.5.1	All	All	All
Operating System	Xen	Xen	All	All	All	All

References						
Reference						Source
[security-announce] SUSE-SU-2015:1409-1: important: Security update for						SUSE
Red Hat Customer Portal						MISC
Red Hat Customer Portal						REDHAT
XSA-138 - Xen Security Advisories						CONFIRM
Debian -- Security Information -- DSA-3348-1 qemu						DEBIAN
QEMU CVE-2015-5154 Heap Based Buffer Overflow Vulnerability						BID
Bug 1243563 – CVE-2015-5154 qemu: ide: atapi: heap overflow during I/O buffer memory access						MISC
[SECURITY] Fedora 23 Update: xen-4.5.1-5.fc23						FEDORA
QEMU IDE Heap Overflow Lets Local Users on a Guest System Gain Elevated Privileges on the Host System - SecurityTracker						SECTRAC
[security-announce] SUSE-SU-2015:1782-1: important: Security update for						SUSE
[security-announce] SUSE-SU-2015:1643-1: important: Security update for						SUSE
[security-announce] SUSE-SU-2015:1302-1: important: Security update for						SUSE
CVE-2015-5154 - Red Hat Customer Portal						MISC
Red Hat Customer Portal						MISC
[SECURITY] Fedora 22 Update: xen-4.5.1-5.fc22						FEDORA
Citrix XenServer Security Update for CVE-2015-5154						CONFIRM
Red Hat Customer Portal						REDHAT
Red Hat Customer Portal						MISC
Xen: Multiple vulnerabilities (GLSA 201604-03) — Gentoo Security						GENTOO
[security-announce] SUSE-SU-2015:1299-1: important: Security update for						SUSE
Red Hat Customer Portal						REDHAT
[security-announce] SUSE-SU-2015:1426-1: important: Security update for						SUSE
[SECURITY] Fedora 21 Update: xen-4.4.2-9.fc21						FEDORA
[security-announce] SUSE-SU-2015:1421-1: important: Security update for						SUSE
QEMU: Arbitrary code execution (GLSA 201510-02) — Gentoo Security						GENTOO
[security-announce] SUSE-SU-2015:1455-1: important: Security update for						SUSE

[security-announce] SUSE-SU-2015:1455-1: Important: Security update for	SUSE
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.	

© [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](#).

Free CVE JSON API [cve.report/api](#)

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