



CVE-2015-5158

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

Summary

CVE	CVE-2015-5158
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-12 01:59:00 UTC
Updated	2020-09-08 13:54:00 UTC
Description	Stack-based buffer overflow in hw/scsi/scsi-bus.c in QEMU, when built with SCSI-device emulation support, allows guest O

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	2.4.0	-	All	All
Application	Qemu	Qemu	2.4.0	rc1	All	All
Application	Qemu	Qemu	2.4.0	rc2	All	All
Application	Qemu	Qemu	All	All	All	All
Application	Qemu	Qemu	2.4.0	-	All	All
Application	Qemu	Qemu	2.4.0	rc1	All	All
Application	Qemu	Qemu	2.4.0	rc2	All	All

References

Reference
[Qemu-devel] [PATCH] scsi: fix buffer overflow in scsi_req_parse_cdb (CV
Qemu CVE-2015-5158 Local Denial of Service Vulnerability
QEMU SCSI Emulation Buffer Overflow Lets Local Users on a Guest System Cause Denial of Service Conditions on the Host System - Securi
QEMU: Arbitrary code execution (GLSA 201510-02) — Gentoo Security
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](#).

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

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