

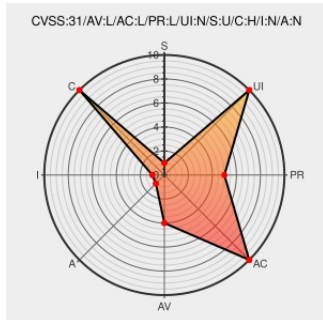


CVE-2016-5337

Published on: 06/14/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:23:00 PM UTC

CVE-2016-5337

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The megasas_ctrl_get_info function in hw/scsi/megasas.c in QEMU allows local guest OS administrators to obtain sensitive host memory information via vectors related to reading device control information.

CVE-2016-5337 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
[SECURITY] [DLA 1599-1] qemu security update	Mailing List Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20181130 [SECURITY] [DLA 1599-1] qemu security update

USN-3047-1: QEMU vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-3047-1
[Qemu-devel] [PULL 06/13] scsi: megasas: null terminate bios version buf	Mailing List Patch Third Party Advisory lists.gnu.org text/x-diff	 MLIST [qemu-devel] 20160607 [PULL 06/13] scsi: megasas: null terminate bios version buffer
oss-security - Re: CVE Request Qemu: scsi: megasas: information leakage in megasas_ctrl_get_info	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20160608 Re: CVE Request Qemu: scsi: megasas: information leakage in megasas_ctrl_get_info
USN-3047-2: QEMU regression Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-3047-2
QEMU 'megasas_ctrl_get_info()' Information Disclosure Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 91097
git.qemu.org Git - qemu.git/commit	git.qemu.org text/xml	 MISC git.qemu.org/?p=qemu.git%3Ba=commit%3Bh=844864fbae66935951529408831c2f22367a57b6
QEMU: Multiple vulnerabilities (GLSA 201609-01) — Gentoo security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201609-01
oss-security - CVE Request Qemu: scsi: megasas: information leakage in megasas_ctrl_get_info	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20160608 CVE Request Qemu: scsi: megasas: information leakage in megasas_ctrl_get_info

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All

Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Qemu	Qemu	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:a:qemu:qemu:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)