

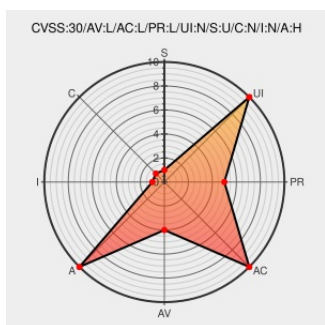


CVE-2018-18849

Published on: 03/17/2019 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:55:00 AM UTC

CVE-2018-18849

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

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

In Qemu 3.0.0, lsi_do_msgin in hw/scsi/lsi53c895a.c allows out-of-bounds access by triggering an invalid msg_len value.

CVE-2018-18849 has been assigned by [M](#) cve@mitre.org 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	NONE	NONE	HIGH

CVSS2 Score: **2.1 - LOW**

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

CVE References

Description	Tags	Link
oss-security - CVE-2018-18849 Qemu: lsi53c895a: OOB msg buffer access leads to DoS	Mailing List Patch Third Party Advisory www.openwall.com text/html	MISC www.openwall.com/lists/oss-security/2018/11/01/1

[Qemu-devel] [PATCH v3] lsi53c895a: check message length value is valid	Patch Third Party Advisory lists.gnu.org text/x-diff	 MISC lists.gnu.org/archive/html/qemu-devel/2018-10/msg06401.html
[SECURITY] Fedora 29 Update: qemu-3.0.0-2.fc29 - package-announce - Fedora Mailing-Lists	Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2018-87f2ace20d
USN-3826-1: QEMU vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3826-1
March 2019 QEMU Vulnerabilities in NetApp Products NetApp Product Security	Third Party Advisory security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20190411-0006/
[security-announce] openSUSE-SU-2018:4004-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2018:4004
[SECURITY] [DLA 1781-1] qemu security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20190509 [SECURITY] [DLA 1781-1] qemu security update
[security-announce] openSUSE-SU-2018:4147-1: moderate: Security update f	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2018:4147
Debian -- Security Information -- DSA-4454-1 qemu	www.debian.org Deprecated Link text/html	 DEBIAN DSA-4454
[security-announce] openSUSE-SU-2018:4111-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2018:4111
Bugtraq: [SECURITY] [DSA 4454-1] qemu security update	seclists.org text/html	 BUGTRAQ 20190531 [SECURITY] [DSA 4454-1] qemu security update

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	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating	Canonical	Ubuntu Linux	14.04	All	All	All

System						
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Application	Qemu	Qemu	3.0.0	All	All	All
Application	Qemu	Qemu	3.0.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:18.10:*****:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:18.10:*****:						
cpe:2.3:o:fedoraproject:fedora:29:*****:						
cpe:2.3:o:fedoraproject:fedora:29:*****:						
cpe:2.3:o:opensuse:leap:15.0:*****:						
cpe:2.3:o:opensuse:leap:42.3:*****:						
cpe:2.3:o:opensuse:leap:15.0:*****:						
cpe:2.3:o:opensuse:leap:42.3:*****:						
cpe:2.3:a:qemu:qemu:3.0.0:*****:						

cpe:2.3:a:qemu:qemu:3.0.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023   |

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](#)