

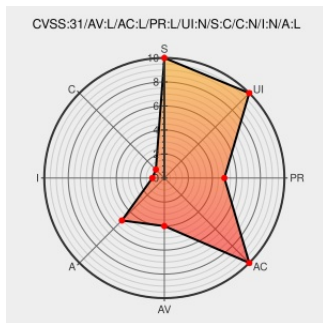


CVE-2019-12068

Published on: 09/24/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:41 PM UTC

CVE-2019-12068

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

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

In QEMU 1:4.1-1, 1:2.1+dfsg-12+deb8u6, 1:2.8+dfsg-6+deb9u8, 1:3.1+dfsg-8~deb10u1, 1:3.1+dfsg-8+deb10u2, and 1:2.1+dfsg-12+deb8u12 (fixed), when executing script in lsi_execute_script(), the LSI scsi adapter emulator advances 's->dsp' index to read next opcode. This can lead to an infinite loop if the next opcode is empty.

Move the existing loop exit after 10k iterations so that it covers no-op opcodes as well.

CVE-2019-12068 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as [LOW](#) severity.

CVSS3 Score: [3.8 - LOW](#)

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

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
[SECURITY] [DLA 1927-1] qemu security update	Mailing List Third Party Advisory	MLIST [debian-lts-announce] 20190920 [SECURITY] [DLA 1927-1] qemu security update

	lists.debian.org text/html	
[security-announce] openSUSE-SU-2019:2510-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2019:2510
git.qemu.org Git - qemu.git/commit	Mailing List Vendor Advisory git.qemu.org text/xml	 MISC git.qemu.org/?p=qemu.git;a=commit;h=de594e47659029316bbf9391efb79da0a1a08e08
[security-announce] openSUSE-SU-2019:2505-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2019:2505
[SECURITY] [DLA 2288-1] qemu security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20200726 [SECURITY] [DLA 2288-1] qemu security update
CVE-2019-12068	Third Party Advisory security-tracker.debian.org text/html	 MISC security-tracker.debian.org/tracker/CVE-2019-12068
[Qemu-devel] [PATCH v3 1/2] scsi: lsi: exit infinite loop while executin	Mailing List Patch Third Party Advisory lists.gnu.org text/x-diff	 MISC lists.gnu.org/archive/html/qemu-devel/2019-08/msg01518.html
USN-4191-1: QEMU vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4191-1
Debian -- Security Information -- DSA-4665-1 qemu	www.debian.org Deprecated Link text/html	 DEBIAN DSA-4665
USN-4191-2: QEMU vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4191-2
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	19.04	All	All	All

Operating System	Canonical	Ubuntu Linux	19.10	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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Qemu	Qemu	1	2.1+dfsg-12+deb8u6	All	All
Application	Qemu	Qemu	1	2.8+dfsg-6+deb9u8	All	All
Application	Qemu	Qemu	1	3.1+dfsg-8+deb10u2	All	All
Application	Qemu	Qemu	1	3.1+dfsg-8~deb10u1	All	All
Application	Qemu	Qemu	1	4.1-1	All	All
Application	Qemu	Qemu	1\	2.1\+dfsg-12\+deb8u6	All	All
Application	Qemu	Qemu	1\	2.8\+dfsg-6\+deb9u8	All	All
Application	Qemu	Qemu	1\	3.1\+dfsg-8\+deb10u2	All	All
Application	Qemu	Qemu	1\	3.1\+dfsg-8\~deb10u1	All	All
Application	Qemu	Qemu	1\	4.1-1	All	All
Application	Qemu	Qemu	1\	2.1\+dfsg-12\+deb8u6	All	All

Application	Qemu	Qemu	1\	2.8\+dfsg-6\+deb9u8	All	All
Application	Qemu	Qemu	1\	3.1\+dfsg-8\+deb10u2	All	All
Application	Qemu	Qemu	1\	3.1\+dfsg-8\~deb10u1	All	All
Application	Qemu	Qemu	1\	4.1-1	All	All
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:18.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:						
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:18.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.0:*:*:*:*:*:						
cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:						
cpe:2.3:a:qemu:qemu:1:2.1+dfsg-12+deb8u6:*:*:*:*:						
cpe:2.3:a:qemu:qemu:1:2.8+dfsg-6+deb9u8:*:*:*:*:						
cpe:2.3:a:qemu:qemu:1:3.1+dfsg-8+deb10u2:*:*:*:*:						
cpe:2.3:a:qemu:qemu:1:3.1+dfsg-8~deb10u1:*:*:*:*:						
cpe:2.3:a:qemu:qemu:1:4.1-1:*:*:*:*:						

cpe:2.3:a:qemu:qemu:1\2.1+dfsg-12\+deb8u6:~:~:~:~:~:~:
cpe:2.3:a:qemu:qemu:1\2.8+dfsg-6\+deb9u8:~:~:~:~:~:~:
cpe:2.3:a:qemu:qemu:1\3.1+dfsg-8\+deb10u2:~:~:~:~:~:~:
cpe:2.3:a:qemu:qemu:1\3.1+dfsg-8\~deb10u1:~:~:~:~:~:~:
cpe:2.3:a:qemu:qemu:1\4.1-1:~:~:~:~:~:~:
cpe:2.3:a:qemu:qemu:1\2.1+dfsg-12\+deb8u6:~:~:~:~:~:~:
cpe:2.3:a:qemu:qemu:1\2.8+dfsg-6\+deb9u8:~:~:~:~:~:~:
cpe:2.3:a:qemu:qemu:1\3.1+dfsg-8\+deb10u2:~:~:~:~:~:~:
cpe:2.3:a:qemu:qemu:1\3.1+dfsg-8\~deb10u1:~:~:~:~:~:~:
cpe:2.3:a:qemu:qemu:1\4.1-1:~:~:~:~:~:~:

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