

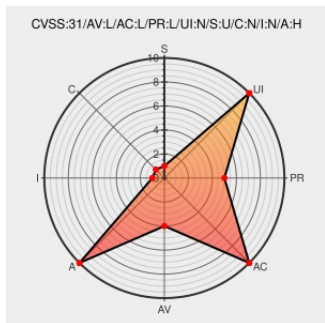


CVE-2018-19364

Published on: 12/13/2018 12:00:00 AM UTC

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

CVE-2018-19364

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

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

hw/9pfs/cofile.c and hw/9pfs/9p.c in QEMU can modify an fid path while it is being accessed by a second thread, leading to (for example) a use-after-free outcome.

CVE-2018-19364 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-2018-19364 Qemu: 9pfs: Use-after-free due to race condition while updating fid path	Mailing List Patch Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20181120 CVE-2018-19364 Qemu: 9pfs: Use-after-free due to race condition while updating fid path

[SECURITY] Fedora 29 Update: qemu-3.0.0-4.fc29 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2019-88a98ce795
[security-announce] openSUSE-SU-2019:1074-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2019:1074
[Qemu-devel] [PATCH] 9p: write lock path in v9fs_co_open2()	Mailing List Patch Vendor Advisory lists.gnu.org text/x-diff	 MLIST [qemu-devel] 20181107 [PATCH] 9p: write lock path in v9fs_co_open2()
[Qemu-devel] [PATCH] 9p: take write lock on fid path updates	Mailing List Patch Vendor Advisory lists.gnu.org text/x-diff	 MLIST [qemu-devel] 20181115 [PATCH] 9p: take write lock on fid path updates
USN-3826-1: QEMU vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-3826-1
[SECURITY] [DLA 1646-1] qemu security update	Mailing List Third Party Advisory lists.debian.org text/html	 MLIST [debian-lts-announce] 20190129 [SECURITY] [DLA 1646-1] qemu security update
Debian -- Security Information -- DSA-4454-1 qemu	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4454
Bugtraq: [SECURITY] [DSA 4454-1] qemu security update	Mailing List Third Party Advisory 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	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	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	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Application	Qemu	Qemu	3.1.0	rc0	All	All
Application	Qemu	Qemu	3.1.0	rc1	All	All
Application	Qemu	Qemu	3.1.0	rc0	All	All
Application	Qemu	Qemu	3.1.0	rc1	All	All
Application	Qemu	Qemu	All	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:debian:debian_linux:8.0:***:***:***:						
cpe:2.3:o:debian:debian_linux:9.0:***:***:***:						

cpe:2.3:o:debian:debian_linux:8.0:*****:
cpe:2.3:o:debian:debian_linux:9.0:*****:
cpe:2.3:o:fedoraproject:fedora:29:*****:
cpe:2.3:o:fedoraproject:fedora:29:*****:
cpe:2.3:o:opensuse:leap:42.3:*****:
cpe:2.3:o:opensuse:leap:42.3:*****:
cpe:2.3:a:qemu:qemu:3.1.0:rc0:*****:
cpe:2.3:a:qemu:qemu:3.1.0:rc1:*****:
cpe:2.3:a:qemu:qemu:3.1.0:rc0:*****:
cpe:2.3:a:qemu:qemu:3.1.0:rc1:*****:
cpe:2.3:a:qemu:qemu:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)