

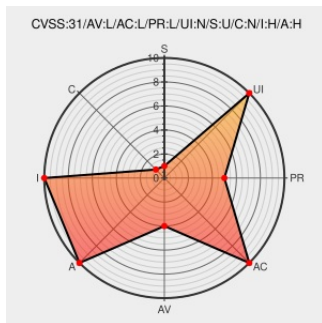


CVE-2019-15791

Published on: 04/23/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

CVE-2019-15791

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

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

In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, `shiftfs_btrfs_ioctl_fd_replace()` installs an fd referencing a file from the lower filesystem without taking an additional reference to that file. After the btrfs ioctl completes this fd is closed, which then puts a reference to that file, leading to a refcount

underflow.

CVE-2019-15791 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Ubuntu - Shiftfs in the Linux kernel** version $\geq 5.3.0-11.12$

Affected Vendor/Software: **Ubuntu - Shiftfs in the Linux kernel** version $< 5.3.0-22.24$

Affected Vendor/Software: **Ubuntu - Shiftfs in the Linux kernel** version $< 5.0.0-35.38$

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

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

CVE References

Description	Tags	Link
USN-4184-1: Linux kernel vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 MISC usn.ubuntu.com/usn/usn-4184-1
USN-4183-1: Linux kernel vulnerabilities Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 MISC usn.ubuntu.com/usn/usn-4183-1
~ubuntu-kernel/ubuntu/+source/linux/+git/eoan - [no description]	Mailing List Patch Third Party Advisory git.launchpad.net text/html	 MISC git.launchpad.net/~ubuntu-kernel/ubuntu/+source/linux/+git/eoan/commit/?id=601a64857b3d7040ca15c39c929e6b9db3373ec1

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	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	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	Linux	Linux Kernel	5.0	All	All	All
Operating System	Linux	Linux Kernel	5.3	All	All	All
Operating System	Linux	Linux Kernel	5.0	All	All	All
Operating System	Linux	Linux Kernel	5.3	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:.*:.*:.*

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:.*:.*:.*

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:.*:.*:.*

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:.*:.*:.*

cpe:2.3:o:linux:linux_kernel:5.0:*****:
cpe:2.3:o:linux:linux_kernel:5.3:*****:
cpe:2.3:o:linux:linux_kernel:5.0:*****:
cpe:2.3:o:linux:linux_kernel:5.3:*****:

Discovery Credit

Jann Horn of Google Project Zero

← Previous ID

Next ID →