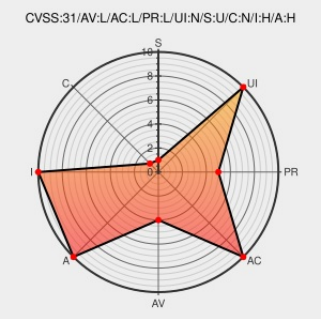
CVE-2019-15794

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

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

CVE-2019-15794

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Overlayfs in the Linux kernel and shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, both replace vma->vm_file in their mmap handlers. On error the original value is not restored, and the reference is put for the file to which vm_file points. On upstream kernels this is not an issue, as no callers dereference vm_file following after call_mmap() returns an error. However, the aufs patchs change mmap_region() to replace the fput() using a local variable with vma_fput(), which will fput() vm_file, leading to a refcount underflow.

CVE-2019-15794 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Ubuntu** - **Linux kernel** version **< 5.3.0-24.26**

Affected Vendor/Software: **Ubuntu** - **Linux kernel** version **< 5.0.0-37.40**

CVSS3 Score: 6.7 - MEDIUM

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
USN-4208-1: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	MISC usn.ubuntu.com/usn/usn-4208-1
USN-4209-1: Linux kernel vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	MISC usn.ubuntu.com/usn/usn-4209-1
~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=270d16ae48a4dbf1c7e25e94cc3e38b4bea37635
~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=ef81780548d20a786cc77ed4203fca146fd81ce3

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	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	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:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:*:*

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

cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:*:*

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→