

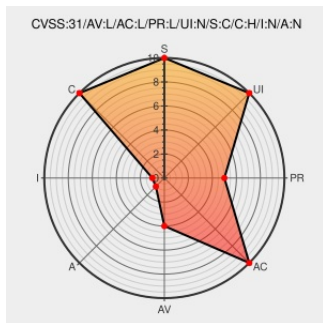


CVE-2019-15793

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

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

CVE-2019-15793

[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, several locations which shift ids translate user/group ids before performing operations in the lower filesystem were translating them into `init_user_ns`, whereas they should have been translated into the `s_user_ns` for the lower filesystem. This

resulted in using ids other than the intended ones in the lower fs, which likely did not map into the shifts `s_user_ns`. A local attacker could use this to possibly bypass discretionary access control permissions.

CVE-2019-15793 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 **>= 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: **8.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

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

impact

PARTIAL

impact

PARTIAL

impact

PARTIAL

CVE References

Description

USN-4184-1: Linux kernel vulnerabilities | Ubuntu security notices

Tags

Third Party Advisory

usn.ubuntu.com

text/html

Link

MISC

 usn.ubuntu.com/usn/usn-4184-1

Description

USN-4183-1: Linux kernel vulnerabilities | Ubuntu security notices

Tags

Third Party Advisory

usn.ubuntu.com

text/html

Link

MISC

 usn.ubuntu.com/usn/usn-4183-1

Description

~ubuntu-kernel/ubuntu/+source/linux/+git/eoan - [no description]

Tags

Mailing List

Patch

Third Party Advisory

git.launchpad.net

text/html

Link

MISC

 git.launchpad.net/~ubuntu-kernel/ubuntu/+source/linux/+git/eoan/commit/?id=3644b9d5688da86f18e017c9c580b75cf52927bb

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:*:*:*:lts:*:*:

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

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

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:*:*:*:*:*:

```
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→

© 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