

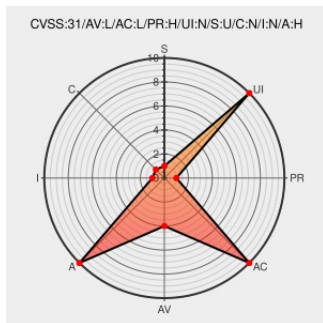


# CVE-2020-11935

Published on: Not Yet Published

Last Modified on: 04/13/2023 06:47:00 PM UTC

## CVE-2020-11935

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

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

It was discovered that aufs improperly managed inode reference counts in the `vfs_sub_dentry_open()` method. A local attacker could use this vulnerability to cause a denial of service attack.

CVE-2020-11935 has been assigned by [security@ubuntu.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Ubuntu](#) - **Linux kernel (aufs filesystem module)** version **!>= 4.4.0-186.216**

Affected Vendor/Software: [Ubuntu](#) - **Linux kernel (aufs filesystem module)** version **!>= 4.15.0-112.113**

Affected Vendor/Software: [Ubuntu](#) - **Linux kernel (aufs filesystem module)** version **!>= 5.4.0-42.46**

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                |

## CVE References

| Description                                                                                          | Tags                                                            | Link                                                  |
|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|-------------------------------------------------------|
| CVE-2020-11935   Ubuntu                                                                              | <a href="#">ubuntu.com</a><br><a href="#">text/html</a>         | <a href="#">UBUNTU Ubuntu Security CVE-2020-11935</a> |
| Bug #1873074 "kernel panic hit by kube-proxy iptables-save/resto..." : Bugs : linux package : Ubuntu | <a href="#">bugs.launchpad.net</a><br><a href="#">text/html</a> | <a href="#">UBUNTU Launchpad Bug 1873074</a>          |

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

There are currently no QIDs associated with this CVE

#### Known Affected Configurations (CPE V2.3)

| Type                                                  | Vendor                    | Product                      | Version | Update | Edition | Language |
|-------------------------------------------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| Operating System                                      | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 14.04   | All    | All     | All      |
| Operating System                                      | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 16.04   | All    | All     | All      |
| Operating System                                      | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 18.04   | All    | All     | All      |
| Operating System                                      | <a href="#">Canonical</a> | <a href="#">Ubuntu Linux</a> | 20.04   | All    | All     | All      |
| Operating System                                      | <a href="#">Debian</a>    | <a href="#">Debian Linux</a> | 10.0    | All    | All     | All      |
| Operating System                                      | <a href="#">Linux</a>     | <a href="#">Linux Kernel</a> | -       | All    | All     | All      |
| cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*: |                           |                              |         |        |         |          |
| cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:esm:*:*: |                           |                              |         |        |         |          |
| cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*: |                           |                              |         |        |         |          |
| cpe:2.3:o:canonical:ubuntu_linux:20.04:*:*:*:lts:*:*: |                           |                              |         |        |         |          |
| cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:         |                           |                              |         |        |         |          |
| cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:               |                           |                              |         |        |         |          |

#### Discovery Credit

Mauricio Faria de Oliveira discovered that the aufs implementation in the Linux kernel improperly managed inode reference counts in the `vfs_sub_dentry_open()` method. A local attacker could use this vulnerability to cause a denial of service.

[← Previous ID](#)

[Next ID →](#)