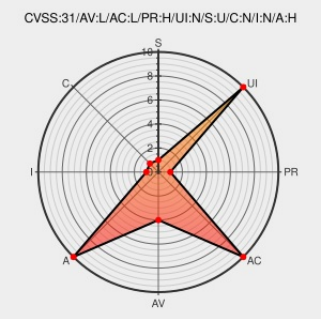
CVE-2020-11935

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 vfsub_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	ubuntu.com text/html	UBUNTU Ubuntu Security CVE-2020-11935
Bug #1873074 “kernel panic hit by kube-proxy iptables-save/resto...” : Bugs : linux package : Ubuntu	bugs.launchpad.net text/html	UBUNTU Launchpad Bug 1873074

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	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Linux	Linux Kernel	-	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 vfsub_dentry_open() method. A local attacker could use this vulnerability to cause a denial of service.

← Previous ID

Next ID→