



CVE-2020-8831

Published on: 04/22/2020 12:00:00 AM UTC

Last Modified on: 10/07/2022 03:38:00 PM UTC

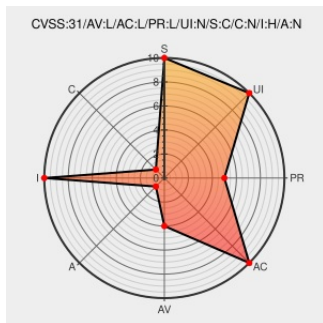
CVE-2020-8831 - advisory for <https://usn.ubuntu.com/4315-1/>

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Apport](#) from [Apport Project](#) contain the following vulnerability:

Apport creates a world writable lock file with root ownership in the world writable `/var/lock/apport` directory. If the `apport/` directory does not exist (this is not uncommon as `/var/lock` is a tmpfs), it will create the directory, otherwise it will simply continue execution using the existing directory. This allows for a symlink attack if an attacker were to create a symlink at `/var/lock/apport`, changing apport's lock file location. This file could then be used to escalate privileges, for example. Fixed in versions 2.20.1-0ubuntu2.23, 2.20.9-0ubuntu7.14, 2.20.11-0ubuntu8.8 and 2.20.11-0ubuntu22.

CVE-2020-8831 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: Canonical - **Apport** version < 2.20.1-0ubuntu2.23

Affected Vendor/Software: Canonical - **Apport** version < 2.20.9-0ubuntu7.14

Affected Vendor/Software: Canonical - **Apport** version < 2.20.11-0ubuntu8.8

Affected Vendor/Software: Canonical - **Apport** version < 2.20.11-0ubuntu22

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	HIGH	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE

cpe:2.3:a:apport_project:apport:-:~::~::~:
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:16.04::~:~::~:
cpe:2.3:o:canonical:ubuntu_linux:18.04::~:~::~:
cpe:2.3:o:canonical:ubuntu_linux:19.10::~:~::~:
cpe:2.3:o:canonical:ubuntu_linux:16.04::~:~::~:
cpe:2.3:o:canonical:ubuntu_linux:18.04::~:~::~:
cpe:2.3:o:canonical:ubuntu_linux:19.10::~:~::~:

Discovery Credit

Maximilien Bourgeteau

Social Mentions

Source	Title	Posted (UTC)
← Previous ID		Next ID→