



CVE-2019-11481

Published on: 02/07/2020 12:00:00 AM UTC

Last Modified on: 06/12/2023 07:15:00 AM UTC

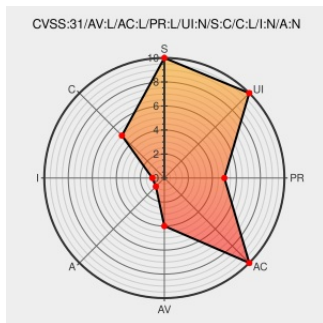
CVE-2019-11481 - advisory for <https://usn.ubuntu.com/usn/usn-4171-1>

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.

CVE-2019-11481 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: Canonical - **apport** version < 2.14.1-0ubuntu3.29+esm2

Affected Vendor/Software: Canonical - **apport** version < 2.20.1-0ubuntu2.20

Affected Vendor/Software: Canonical - **apport** version < 2.20.9-0ubuntu7.8

Affected Vendor/Software: Canonical - **apport** version < 2.20.11-0ubuntu8.1

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **6.1 - MEDIUM**

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

CVE References

Description	Tags	Link
Ubuntu Apport / Whoopsie DoS / Integer Overflow ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/172858/Ubuntu-Apport-Whoopsie-DoS-Integer-Overflow.html
USN-4171-1: Apport vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 MISC usn.ubuntu.com/usn/usn-4171-1
USN-4171-2: Apport vulnerabilities Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 MISC usn.ubuntu.com/usn/usn-4171-2

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
Application	Apport Project	Apport	-	All	All	All
Application	Apport Project	Apport	-	All	All	All
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	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
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	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
cpe:2.3:a:apport_project:apport:-:*****:.*:						
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.*.*.*:lts:*.*.*:
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:19.10.*.*.*.*.*.*:
cpe:2.3:o:canonical:ubuntu_linux:14.04.*.*.*:esm:*.*.*:
cpe:2.3:o:canonical:ubuntu_linux:16.04.*.*.*:lts:*.*.*:
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:19.10.*.*.*.*.*.*:

Discovery Credit

Kevin Backhouse

[← Previous ID](#)

[Next ID →](#)