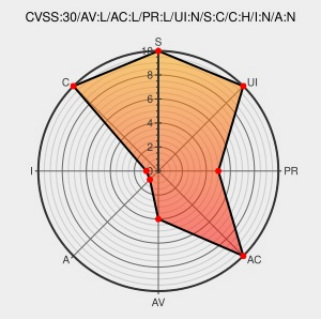
CVE-2019-7307

Published on: 08/29/2019 12:00:00 AM UTC

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

CVE-2019-7307 - advisory for https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-7307.html

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Apport from Apport Project contain the following vulnerability:

Apport before versions 2.14.1-0ubuntu3.29+esm1, 2.20.1-0ubuntu2.19, 2.20.9-0ubuntu7.7, 2.20.10-0ubuntu27.1, 2.20.11-0ubuntu5 contained a TOCTTOU vulnerability when reading the users ~/.apport-ignore.xml file, which allows a local attacker to replace this file with a symlink to any other file on the system and so cause Apport to include the contents of this other file in the resulting crash report. The crash report could then be read by that user either by causing it to be uploaded and reported to Launchpad, or by leveraging some other vulnerability to read the resulting crash report, and so allow the user to read arbitrary files on the system.

CVE-2019-7307 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Ubuntu** - **apport** version **before 2.14.1-0ubuntu3.29+esm1**

Affected Vendor/Software: **Ubuntu** - **apport** version **before 2.20.1-0ubuntu2.19**

Affected Vendor/Software: **Ubuntu** - **apport** version **before 2.20.9-0ubuntu7.7**

Affected Vendor/Software: **Ubuntu** - **apport** version **before 2.20.10-0ubuntu27.1**

Affected Vendor/Software: **Ubuntu** - **apport** version **before 2.20.11-0ubuntu5**

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 4.4 - MEDIUM

CVSS2 Score: 4.4 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	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
Bug #1830858 “TOCTOU vulnerability in _get_ignore_dom (report.py...” : Bugs : apport package : Ubuntu	Exploit Issue Tracking Vendor Advisory bugs.launchpad.net text/html	MISC bugs.launchpad.net/ubuntu/%2Bsource/apport/%2Bbug/1830858
CVE-2019-7307 | Ubuntu	Vendor Advisory people.canonical.com text/html	MISC people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-7307.html

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	2.14.1	All	All	All
Application	Apport Project	Apport	2.20.1	All	All	All
Application	Apport Project	Apport	2.20.10	All	All	All
Application	Apport Project	Apport	2.20.9	All	All	All
Application	Apport Project	Apport	2.14.1	All	All	All
Application	Apport Project	Apport	2.20.1	All	All	All
Application	Apport Project	Apport	2.20.10	All	All	All
Application	Apport Project	Apport	2.20.9	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:2.14.1:*:*:*:*:*:*:*:

cpe:2.3:a:apport_project:apport:2.20.1:*:*:*:*:*:*:*:

cpe:2.3:a:apport_project:apport:2.20.10:*:*:*:*:*:*:*:

cpe:2.3:a:apport_project:apport:2.20.9:*:*:*:*:*:*:*:

cpe:2.3:a:apport_project:apport:2.14.1:*:*:*:*:*:*:*:

cpe:2.3:a:apport_project:apport:2.20.1:*:*:*:*:*:*:*:

cpe:2.3:a:apport_project:apport:2.20.10:*:*:*:*:*:*:*:

cpe:2.3:a:apport_project:apport:2.20.9:*:*:*:*:*:*:*:

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 of Semmle Security Research Team

Kevin Backhouse of Semmle Security Research Team

← Previous ID

Next ID→