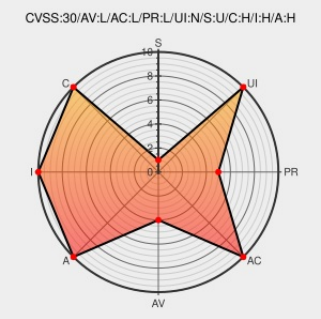
CVE-2017-14180

Published on: 02/02/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:44 PM UTC

CVE-2017-14180

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



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

Apport 2.13 through 2.20.7 does not properly handle crashes originating from a PID namespace allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion or possibly gain root privileges, a different vulnerability than CVE-2017-14179.

CVE-2017-14180 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **na**/ - **Apport** version **2.13 through 2.20.7**

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: 7.2 - HIGH

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

CVE References

Description	Tags	Link
Bug #1726372 “Multiple security issues in Apport” : Bugs :	Issue Tracking	CONFIRM launchpad.net/bugs/1726372

apport package : Ubuntu	Third Party Advisory launchpad.net text/html	
Ubuntu CVE Tracker	Third Party Advisory people.canonical.com text/html	CONFIRM people.canonical.com/~ubuntu-security/cve/?cve=CVE-2017-14180
~apport-hackers/apport/trunk : revision 3171	Issue Tracking Third Party Advisory bazaar.launchpad.net text/xml	CONFIRM bazaar.launchpad.net/~apport-hackers/apport/trunk/revision/3171
USN-3480-1: Apport vulnerabilities | Ubuntu	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-3480-1

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	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	17.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	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	17.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All

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

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:17.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

Discovery Credit

Array

← Previous ID

Next ID→