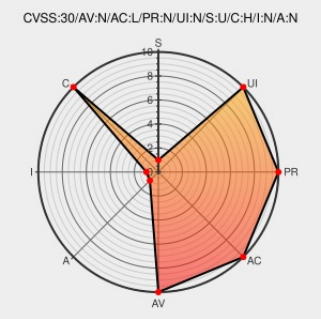
CVE-2017-14178

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

Last Modified on: 03/23/2021 11:26:46 PM UTC

CVE-2017-14178

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



Certain versions of Snapd from Snapcraft contain the following vulnerability:

In snapd 2.27 through 2.29.2 the 'snap logs' command could be made to call journalctl without match arguments and therefore allow unprivileged, unauthenticated users to bypass systemd-journald's access restrictions.

CVE-2017-14178 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
daemon: for /v2/logs, 404 when no services are found by chipaca · Pull Request #4194 · snapcore/snapd · GitHub	Issue Tracking, Third Party Advisory, github.com, text/html	CONFIRM github.com/snapcore/snapd/pull/4194

CVE-2017-14178 | Ubuntu	Patch Vendor Advisory people.canonical.com text/html	CONFIRM people.canonical.com/~ubuntu-security/cve/2017/CVE-2017-14178.html
Bug #1730255 “snapd gives all users access to system logs” : Bugs : snapd package : Ubuntu	Issue Tracking Patch launchpad.net text/html	CONFIRM launchpad.net/bugs/1730255

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snapcraft	Snapd	All	All	All	All

cpe:2.3:a:snapcraft:snapd:*:*:*:*:*:*:*:*:

Discovery Credit

Array

← Previous ID

Next ID→