

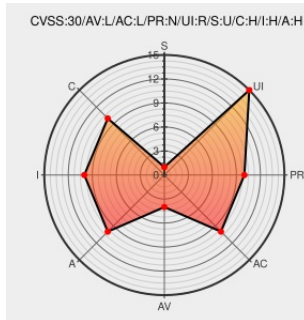


CVE-2017-10708

Published on: 07/18/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:28 PM UTC

CVE-2017-10708

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

An issue was discovered in Apport through 2.20.x. In `apport/report.py`, Apport sets the `ExecutablePath` field and it then uses the path to run package specific hooks without protecting against path traversal. This allows remote attackers to execute arbitrary code via a crafted `.crash` file.

CVE-2017-10708 has been assigned by [M](#) `cve@mitre.org` to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Change log : apport package : Ubuntu	Third Party Advisory launchpad.net text/html	CONFIRM launchpad.net/ubuntu/+source/apport/+changelog

Bug #1700573 "Code execution through path traversal in .crash fi..." : Bugs : Apport

Third Party Advisory

launchpad.net

text/html



CONFIRM launchpad.net/bugs/1700573

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	All
cpe:2.3:a:apport_project:apport:*:*:*:*:*:.*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)