



CVE-2016-9951

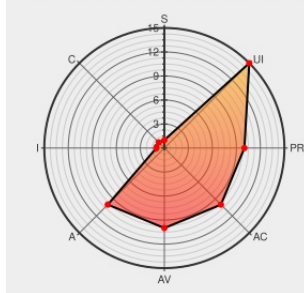
Published on: 12/16/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:17 PM UTC

CVE-2016-9951

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

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H



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

An issue was discovered in Apport before 2.20.4. A malicious Apport crash file can contain a restart command in `RespawnCommand` or `ProcCmdline` fields. This command will be executed if a user clicks the Relaunch button on the Apport prompt from the malicious crash file.

The fix is to only show the Relaunch button on Apport crash files generated by local systems. The Relaunch button will be hidden when crash files are opened directly in Apport-GTK.

CVE-2016-9951 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Bug #1648806 "Arbitrary code execution through crafted CrashDB o..."	Apport Project	MISC

Bug #1648806 Arbitrary code execution through crafted CrashDB 0... : Bugs : Apport	Issue Tracking Patch bugs.launchpad.net text/html	 MISC bugs.launchpad.net/apport/+bug/1648806
Apport Multiple Security Vulnerabilities	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 95011
Reliably compromising Ubuntu desktops by attacking the crash reporter Donncha O'Cearbhaill	Exploit Technical Description Third Party Advisory donncha.is text/html	 MISC donncha.is/2016/12/compromising-ubuntu-desktop/
GitHub - DonnchaC/ubuntu-apport-exploitation: This project contains a PoC and exploit generator for a code execution bug in Ubuntu's Apport crash reporter	Issue Tracking Third Party Advisory github.com text/html	 MISC github.com/DonnchaC/ubuntu-apport-exploitation
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution - Linux local Exploit	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 40937
USN-3157-1: Apport vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-3157-1

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 →](#)