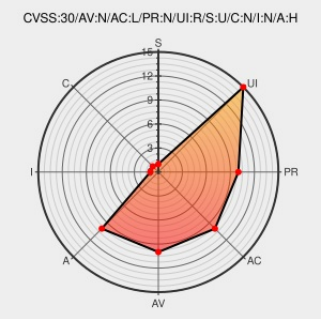
# CVE-2016-9951

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




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 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 c...” : | | MISC |

| | | |
|---|---|---|
| Bug #1648806 "Arbitrary code execution through crafted CrashDB o... " : Bugs : Apport | Issue Tracking<br>Patch<br>bugs.launchpad.net<br>text/html | MISC<br>bugs.launchpad.net/apport/+bug/1648806 |
| Apport Multiple Security Vulnerabilities | Third Party Advisory<br>VDB Entry<br>cve.report (archive)<br>text/html | BID 95011 |
| Reliably compromising Ubuntu desktops by attacking the crash reporter \| Donncha O'Cearbhaill | Exploit<br>Technical Description<br>Third Party Advisory<br>donncha.is<br>text/html | MISC<br>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<br>Third Party Advisory<br>github.com<br>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<br>Proof of Concept<br>text/html | EXPLOIT-DB 40937 |
| USN-3157-1: Apport vulnerabilities \| Ubuntu | www.ubuntu.com<br>text/html | UBUNTU USN-3157-1 |



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 |

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→