



CVE-2015-1338

Published on: 10/01/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:09 PM UTC

CVE-2015-1338

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

kernel_crashdump in Apport before 2.19 allows local users to cause a denial of service (disk consumption) or possibly gain privileges via a (1) symlink or (2) hard link attack on /var/crash/vmcore.log.

CVE-2015-1338 has been assigned by security@ubuntu.com to track the vulnerability

CVSS2 Score: **7.2 - HIGH**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Apport 2.19 (Ubuntu 15.04) - Local
Privilege Escalation - Linux local
Exploit

[Exploit](#)
[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 38353](#)

2.19 : Series trunk : Apport

[Patch](#)
[launchpad.net](#)
[text/html](#)

[CONFIRM launchpad.net/apport/trunk/2.19](#)

Full Disclosure: Apport
kernel_crashdump symlink
vulnerability exploitation

[seclists.org](#)
[text/html](#)

[FULLDISC 20150927 Apport kernel_crashdump symlink vulnerability exploitation](#)

Apport Kernel Crashdump File
Access Vulnerabilities

[Exploit](#)
[www.halfdog.net](#)
[text/xml](#)

[MISC](#)
[www.halfdog.net/Security/2015/ApportKernelCrashdumpFileAccessVulnerabilities](#)

USN-2744-1: Apport vulnerability | Ubuntu

[www.ubuntu.com](#)
[text/html](#)

 UBUNTU USN-2744-1

Ubuntu Apport kernel_crashdump
Symlink ≈ Packet Storm

[Exploit](#)
[packetstormsecurity.com](#)
[text/html](#)

 MISC [packetstormsecurity.com/files/133723/Ubuntu-Apport-kernel_crashdump-Symlink.html](#)

Bug #1492570
"/usr/share/apport/kernel_crashdump
accesses files ...": Bugs : apport
package : Ubuntu

[bugs.launchpad.net](#)
[text/html](#)

 CONFIRM [bugs.launchpad.net/ubuntu/+source/apport/+bug/1492570](#)

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
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
cpe:2.3:a:apport_project:apport:*.***:***:.*						
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:***:.*:.*						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:***:.*:.*						
cpe:2.3:o:canonical:ubuntu_linux:15.04:***:***:.*:.*						
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:***:.*:.*						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:***:.*:.*						
cpe:2.3:o:canonical:ubuntu_linux:15.04:***:***:.*:.*						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)