



CVE-2019-15790

Published on: 04/27/2020 12:00:00 AM UTC

Last Modified on: 06/12/2023 07:15:00 AM UTC

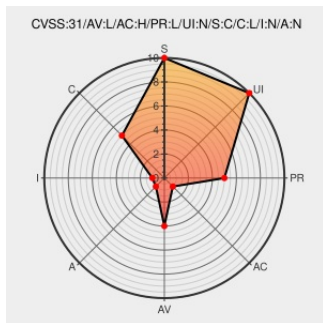
CVE-2019-15790 - advisory for <https://usn.ubuntu.com/4171-1/>

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Apport reads and writes information on a crashed process to `/proc/pid` with elevated privileges. Apport then determines which user the crashed process belongs to by reading `/proc/pid` through `get_pid_info()` in `data/apport`. An unprivileged user could exploit this to read information about a privileged running process by exploiting PID

recycling. This information could then be used to obtain ASLR offsets for a process with an existing memory corruption vulnerability. The initial fix introduced regressions in the Python Apport library due to a missing argument in `Report.add_proc_envron` in `apport/report.py`. It also caused an `autopkgtest` failure when reading `/proc/pid` and with Python 2 compatibility by reading `/proc` maps. The initial and subsequent regression fixes are in 2.20.11-0ubuntu16, 2.20.11-0ubuntu8.6, 2.20.9-0ubuntu7.12, 2.20.1-0ubuntu2.22 and 2.14.1-0ubuntu3.29+esm3.

CVE-2019-15790 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as **LOW** severity.

Affected Vendor/Software: Canonical - Apport version < 2.14.1-0ubuntu3.29+esm3

Affected Vendor/Software: Canonical - Apport version < 2.20.1-0ubuntu2.22

Affected Vendor/Software: Canonical - Apport version < 2.20.9-0ubuntu7.12

Affected Vendor/Software: Canonical - Apport version < 2.20.11-0ubuntu8.6

Affected Vendor/Software: Canonical - Apport version < 2.20.11-0ubuntu16

CVSS3 Score: **3.3 - LOW**

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

CVSS2 Score: 2.1 - LOW

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

Ubuntu Apport / Whoopsie DoS / Integer Overflow ≈
Packet Stormpacketstormsecurity.com
text/htmlMISC packetstormsecurity.com/files/172858/Ubuntu-
Apport-Whoopsie-DoS-Integer-Overflow.htmlBug #1854237 "autopkgtests fail after security fixes" :
Bugs : ApportIssue Tracking
Third Party Advisory
bugs.launchpad.net
text/html

CONFIRM bugs.launchpad.net/apport/+bug/1854237

USN-4171-4: Apport regression | Ubuntu security
noticesThird Party Advisory
usn.ubuntu.com
text/html

CONFIRM usn.ubuntu.com/4171-4/

USN-4171-1: Apport vulnerabilities | Ubuntu security
noticesThird Party Advisory
usn.ubuntu.com
text/html

CONFIRM usn.ubuntu.com/4171-1/

Bug #1851806 "'module' object has no attribute
'O_PATH'" : Bugs : apport package : UbuntuExploit
Issue Tracking
Third Party Advisory
bugs.launchpad.net
text/htmlCONFIRM
bugs.launchpad.net/ubuntu/+source/apport/+bug/1851806USN-4171-2: Apport vulnerabilities | Ubuntu security
noticesThird Party Advisory
usn.ubuntu.com
text/html

CONFIRM usn.ubuntu.com/4171-2/

Bug #1850929 "python3-apport regression: missing
argument in Rep..." : Bugs : apport package : UbuntuExploit
Issue Tracking
Patch
Third Party Advisory
bugs.launchpad.net
text/htmlCONFIRM
bugs.launchpad.net/ubuntu/+source/apport/+bug/1850929Bug #1839795 "PID recycling enables an
unprivileged user to gene..." : Bugs : apport package
: UbuntuExploit
Issue Tracking
Third Party Advisory
bugs.launchpad.net
text/htmlCONFIRM
bugs.launchpad.net/ubuntu/+source/apport/+bug/1839795USN-4171-5: Apport regression | Ubuntu security
noticesThird Party Advisory
usn.ubuntu.com
text/html

CONFIRM usn.ubuntu.com/4171-5/

USN-4171-3: Apport regression | Ubuntu security
noticesThird Party Advisory
usn.ubuntu.com
text/html

CONFIRM usn.ubuntu.com/4171-3/

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
Application	Apport Project	Apport	-	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
cpe:2.3:a:apport_project:apport:-:*:*:*:*:*:						
cpe:2.3:a:apport_project:apport:-:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:						

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*

cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*

Discovery Credit

Kevin Backhouse

← Previous ID

Next ID→

© 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](#)