



CVE-2019-18198

Published on: 10/18/2019 12:00:00 AM UTC

Last Modified on: 01/20/2023 06:48:00 PM UTC

CVE-2019-18198

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

In the Linux kernel before 5.3.4, a reference count usage error in the fib6_rule_suppress() function in the fib6 suppression feature of net/ipv6/fib6_rules.c, when handling the FIB_LOOKUP_NOREF flag, can be exploited by a local attacker to corrupt memory, aka CID-ca7a03c41753.

CVE-2019-18198 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	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
ipv6: do not free rt if FIB_LOOKUP_NOREF is set on suppress rule · torvalds/linux@ca7a03c4175366a92cee0ccc4fec0038c3266e26 · GitHub	Patch Third Party Advisory github.com	MISC github.com/torvalds/linux/commit/ca7a03c4175366a92cee0ccc4fec0038c3266e26

torvalds/linux@ca7a03c · GitHub	text/html	
	Release Notes Vendor Advisory cdn.kernel.org text/plain	 MISC cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.3.4
USN-4161-1: Linux kernel vulnerability Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4161-1
Bug #1847478 "eoan kernel does not contain "ipv6: do not free rt..." : Bugs : linux package : Ubuntu	Exploit Issue Tracking Third Party Advisory launchpad.net text/html	 MISC launchpad.net/bugs/1847478
October 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20191031-0005/
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	 MISC git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ca7a03c4175366a92cee0ccc4fec0038c3266e26

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
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:19.10:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:						

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](#)