



CVE-2019-19050

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-19050
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-18 06:15:00 UTC
Updated	2023-11-07 03:07:00 UTC
Description	A memory leak in the crypto_reportstat() function in crypto/crypto_user_stat.c in the Linux kernel through 5.3.11 allows att

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Broadcom	Fabric Operating System	-	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.5	rc1	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Hardware	Netapp	Aff A400	-	All	All	All
Operating System	Netapp	Aff A400 Firmware	-	All	All	All
Hardware	Netapp	Aff A700s	-	All	All	All
Operating System	Netapp	Aff A700s Firmware	-	All	All	All
Operating System	Netapp	Brocade Fabric Os	-	All	All	All
Application	Netapp	Data Availability Services	-	All	All	All
Application	Netapp	E-series Santricity Os Controller	All	All	All	All
Hardware	Netapp	Fas8300	-	All	All	All

Operating System	Netapp	Fas8300 Firmware	-	All	All	All
Hardware	Netapp	Fas8700	-	All	All	All
Operating System	Netapp	Fas8700 Firmware	-	All	All	All
Hardware	Netapp	H610s	-	All	All	All
Operating System	Netapp	H610s Firmware	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Hardware	Netapp	Hci Storage Node	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All

References

Reference	Source	Link
November 2019 Linux Kernel Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
USN-4284-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
[SECURITY] Fedora 31 Update: kernel-5.3.12-300.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
USN-4258-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com
[SECURITY] Fedora 30 Update: kernel-5.3.12-200.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Kernel Live Patch Security Notice LSN-0063-1 ~ Packet Storm	MISC	packetstormsecurity.com
[SECURITY] Fedora 30 Update: kernel-5.3.12-200.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
crypto: user - fix memory leak in crypto_reportstat · torvalds/linux@c03b04d · GitHub	MISC	github.com
[SECURITY] Fedora 31 Update: kernel-5.3.12-300.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

CVE.report and Source URL Uptime Status status.cve.report