



CVE-2020-25212

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

Summary

CVE	CVE-2020-25212
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-09 16:15:00 UTC
Updated	2022-04-28 18:32:00 UTC
Description	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt me

Risk And Classification

Problem Types: CWE-787 | CWE-367

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	20.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:1655-1: important: Security update	SUSE	lists.opensuse.org	
USN-4578-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
[SECURITY] [DLA 2420-2] linux regression update	MLIST	lists.debian.org	
[security-announce] openSUSE-SU-2020:1698-1: important: Security update	SUSE	lists.opensuse.org	
grsecurity on Twitter: "https://t.co/kiTL438tB1"	MISC	twitter.com	Third Party Advisory

[security-announce] openSUSE-SU-2020:1682-1: important: Security update	SUSE	lists.opensuse.org	
[SECURITY] [DLA 2385-1] linux-4.19 security update	MLIST	lists.debian.org	
USN-4527-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Mailing List, Patch, Vendor A
USN-4525-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.8.3	MISC	cdn.kernel.org	Mailing List, Vendor Advisor
[SECURITY] [DLA 2420-1] linux security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159185](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1578)

[239314](#) Red Hat Update for kernel-rt (RHSA-2021:1739)

[239339](#) Red Hat Update for kernel (RHSA-2021:1578)

[353100](#) Amazon Linux Security Advisory for kernel : ALAC2012-2021-024

[353101](#) Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025

[353102](#) Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026

[353135](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-016

[6140295](#) AWS Bottlerocket Security Update for kernel (GHSA-63hp-p87h-7795)

[750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)

[750533](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2112-1)

[900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91

[903066](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3454)

[906076](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3454-1)

[940354](#) AlmaLinux Security Update for kernel (ALSA-2021:1578)

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](#)