



CVE-2020-25211

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-25211
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-09 16:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	In the Linux kernel through 5.8.7, local attackers able to inject contrack netlink configuration could overflow a local buffer, c

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tag
[SECURITY] Fedora 31 Update: kernel-5.8.9-101.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] [DLA 2420-2] linux regression update	MLIST	lists.debian.org	
Debian -- Security Information -- DSA-4774-1 linux	DEBIAN	www.debian.org	This
[SECURITY] Fedora 32 Update: kernel-5.8.9-200.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	This
[SECURITY] Fedora 31 Update: kernel-5.8.9-101.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	This

grsecurity on Twitter: "Fixed in #grsecurity 6 months ago: https://t.co/TpQt2mMaY8..."	MISC	twitter.com	Thir
[SECURITY] [DLA 2417-1] linux-4.19 security update	MLIST	lists.debian.org	Thir
CVE-2020-25211 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	Thir
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Exp
[SECURITY] Fedora 32 Update: kernel-5.8.9-200.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] [DLA 2420-1] linux security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [239151](#) Red Hat Update for kernel (RHSA-2021:0856)
- [239344](#) Red Hat Update for kernel (RHSA-2021:1531)
- [239456](#) Red Hat Update for kernel-rt (RHSA-2021:0774)
- [257070](#) CentOS Security Update for kernel (CESA-2021:0856)
- [352339](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-029
- [352340](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-028
- [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
- [353134](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-017
- [377038](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)
- [610321](#) Google Pixel Android March 2021 Security Patch Missing
- [6140026](#) AWS Bottlerocket Security Update for kernel (GHSA-x776-q533-gfwx)
- [6140223](#) AWS Bottlerocket Security Update for kernel (GHSA-x776-q533-gfwx)
- [750373](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0241-1)
- [900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [903611](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (2202)
- [906162](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (2202-1)

© [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](#) 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](#)