



CVE-2021-26708

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

Summary

CVE	CVE-2021-26708
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-05 14:15:00 UTC
Updated	2023-11-09 13:57:00 UTC
Description	A local privilege escalation was discovered in the Linux kernel before 5.10.13. Multiple race conditions in the AF_VSOCK in

Risk And Classification

Problem Types: CWE-667

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	500f	-	All	All	All
Hardware	Netapp	A250	-	All	All	All
Application	Netapp	Aff Baseboard Management Controller	-	All	All	All
Hardware	Netapp	Baseboard Management Controller 500f	-	All	All	All
Operating System	Netapp	Baseboard Management Controller 500f Firmware	All	All	All	All
Hardware	Netapp	Baseboard Management Controller A250	-	All	All	All
Operating System	Netapp	Baseboard Management Controller A250 Firmware	All	All	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Application	Netapp	Fas Baseboard Management Controller	-	All	All	All
Hardware	Netapp	Hci H410c	-	All	All	All
Operating System	Netapp	Hci H410c Firmware	-	All	All	All
Application	Netapp	Solidfire Baseboard Management Controller	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All

References

Reference	Source	Link	Tags
oss-security - CVE-2022-0185: Linux kernel slab out-of-bounds write: exploit and writeup	MLIST	www.openwall.com	
oss-security - Re: Linux kernel: Exploitable vulnerabilities in AF_VSOCK implementation	MLIST	www.openwall.com	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.10.13	MISC	cdn.kernel.org	Release Not
CVE-2021-26708 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
oss-security - Linux kernel: Exploitable vulnerabilities in AF_VSOCK implementation	MISC	www.openwall.com	Mailing List,
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Patch, Vende
oss-security - Re: Linux kernel: Exploitable vulnerabilities in AF_VSOCK implementation	MLIST	www.openwall.com	Mailing List,
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159144](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1093)
- [179903](#) Debian Security Update for linux (CVE-2021-26708)
- [239202](#) Red Hat Update for kernel (RHSA-2021:1093)
- [239204](#) Red Hat Update for kernel-rt (RHSA-2021:1081)
- [900098](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [902961](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3879)
- [940387](#) AlmaLinux Security Update for kernel (ALSA-2021:1093)

© 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/cve). This site includes MITRE data granted under the following [license](#).

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