CVE-2022-3541

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-3541
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-17 12:15:00 UTC
Updated	2023-11-07 03:51:00 UTC
Description	A vulnerability classified as critical has been found in Linux Kernel. This affects the function spl2sw_nvmem_get_mac_addr

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Ta
CVE-2022-3541 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
CVE-2022-3541 | Linux Kernel BPF spl2sw_driver.c spl2sw_nvmem_get_mac_address use after free	N/A	vuldb.com	
kernel/git/bpf/bpf-next.git - BPF next kernel tree	N/A	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184668 Debian Security Update for linux (CVE-2022-3541)

199089 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5793-1)

199096 Ubuntu Security Notification for Linux kernel (Azure) Vulnerabilities (USN-5793-2)

199098 Ubuntu Security Notification for Linux kernel (IBM) Vulnerabilities (USN-5793-4)

199099 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5793-3)

904231 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11158)

904271 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11132)

904373 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11158-1)

904428 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11132-1)

905982 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11158-2)

906277 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (11132-2)

© 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 registred 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.

Free CVE JSON API cve.report/api

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