CVE-2023-28866

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

Summary

CVE	CVE-2023-28866
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-27 01:15:00 UTC
Updated	2023-11-07 04:10:00 UTC
Description	In the Linux kernel through 6.2.8, net/bluetooth/hci_sync.c allows out-of-bounds access because amp_init1[] and amp_init2

Risk And Classification

Problem Types: CWE-125

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	Tags
[PATCH] Bluetooth: HCI: Fix global-out-of-bounds - Sungwoo Kim		lore.kernel.org	
[PATCH] Bluetooth: HCI: Fix global-out-of-bounds - Sungwoo Kim	MISC	lore.kernel.org	
pull-request: bluetooth 2023-03-22 - Patchwork	MISC	patchwork.kernel.org	
kernel/git/bluetooth/bluetooth-next.git - Bluetooth kernel development tree	MISC	git.kernel.org	
pull-request: bluetooth 2023-03-22 - Patchwork		patchwork.kernel.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

183548 Debian Security Update for linux (CVE-2023-28866)

199298 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6033-1)

199422 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6175-1)

199437 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6186-1)

907125 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (25911-1)

907186 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (25933-1)

© 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 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**