CVE-2021-38208

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

Summary

CVE	CVE-2021-38208
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-08 20:15:00 UTC
Updated	2021-09-21 18:23:00 UTC
Description	net/nfc/llcp_sock.c in the Linux kernel before 5.12.10 allows local unprivileged users to cause a denial of service (NULL poi

Risk And Classification

Problem Types: CWE-476

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
1992810 – (CVE-2021-38208) CVE-2021-38208 kernel: NULL pointer dereference in net/nfc/llcp_sock.c by making a getsockname call after a
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.10
nfc: fix NULL ptr dereference in llcp_sock_getname() after failed con… · torvalds/linux@4ac06a1 · GitHub
oss-security - Re: Linux kernel: nfc: null ptr dereference in llcp_sock_getname
oss-security - Re: Linux kernel: nfc: null ptr dereference in llcp_sock_getname
oss-security - Re: Linux kernel: nfc: null ptr dereference in llcp_sock_getname
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179869 Debian Security Update for linux (CVE-2021-38208)

198468 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5050-1)

353147 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-004

353158 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002

671051 EulerOS Security Update for kernel (EulerOS-SA-2021-2663)

671134 EulerOS Security Update for kernel (EulerOS-SA-2021-2688)

671137 EulerOS Security Update for kernel (EulerOS-SA-2021-2713)

752120 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1651-1)

752125 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1686-1)

752126 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1687-1)

752231 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2082-1)

752237 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2083-1)

752240 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2103-1)

752250 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2111-1)

753176 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1676-1)

753299 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1669-1)

900294 CBL-Mariner Linux Security Update for kernel 5.10.52.1

900304 CBL-Mariner Linux Security Update for kernel 5.10.57.1

900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1

901779 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6592-1)

903572 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5083)

905782 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5083-1)

© 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**