



CVE-2020-26088

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

Summary

CVE	CVE-2020-26088
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-24 15:15:00 UTC
Updated	2022-04-27 18:48:00 UTC
Description	A missing CAP_NET_RAW check in NFC socket creation in net/nfc/rawsock.c in the Linux kernel before 5.8.2 could be use

Risk And Classification

Problem Types: CWE-276

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

References

Reference	Source	Link	Tags
[security-announce] openSUSE-SU-2020:1655-1: important: Security update	SUSE	lists.opensuse.org	
USN-4578-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu	UBUNTU	usn.ubuntu.com	
[SECURITY] [DLA 2420-2] linux regression update	MLIST	lists.debian.org	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.8.2	MISC	cdn.kernel.org	Patch, Release Notes,

[SECURITY] [DLA 2385-1] linux-4.19 security update	MLIST	lists.debian.org	Third Party Advisory
net/nfc/rawsock.c: add CAP_NET_RAW check. · torvalds/linux@26896f0 · GitHub	MISC	github.com	Patch, Third Party Advisory
[SECURITY] [DLA 2420-1] linux security update	MLIST	lists.debian.org	
[security-announce] openSUSE-SU-2020:1586-1: important: Security update	SUSE	lists.opensuse.org	Third Party Advisory
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

[750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)

[900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91

[903558](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3499)

[906100](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3499-1)

© [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](#)