



CVE-2020-10942

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

Summary

CVE	CVE-2020-10942
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-24 22:15:00 UTC
Updated	2022-04-22 19:06:00 UTC
Description	In the Linux kernel before 5.5.8, get_raw_socket in drivers/vhost/net.c lacks validation of an sk_family field, which might allow

Risk And Classification

Problem Types: CWE-787

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	Canonical	Ubuntu Linux	19.10	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	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	15.1	All	All	All

References

Reference	Source	Link
USN-4364-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
[security-announce] openSUSE-SU-2020:0543-1: important: Security update	SUSE	lists.opensuse.org
USN-4345-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com

cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.5.8	MISC	cdn.kernel.c
USN-4342-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.
USN-4344-1: Linux kernel vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.
LKML: syzbot: Re: kernel panic: stack is corrupted in vhost_net_ioctl	MISC	lkml.org
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.or
[SECURITY] [DLA 2241-2] linux security update	MLIST	lists.debian.
oss-security - CVE-2020-10942 Kernel: vhost-net: stack overflow in get_raw_socket while checking sk_family field	MLIST	www.openw
Debian -- Security Information -- DSA-4667-1 linux	DEBIAN	www.debian
[SECURITY] [DLA 2242-1] linux-4.9 security update	MLIST	lists.debian.
[SECURITY] [DLA 2241-1] linux security update	MLIST	lists.debian.
Debian -- Security Information -- DSA-4698-1 linux	DEBIAN	www.debian
CVE-2020-10942 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [159684](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)
- [352352](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-016
- [352353](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-015
- [352354](#) Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2020-014
- [377065](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0113)
- [750691](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1141-1)
- [900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [903515](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3511)
- [905901](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3511-1)
- [940256](#) AlmaLinux Security Update for kernel (ALSA-2020:4431)

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](#)