CVE-2022-39190

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-39190
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-02 05:15:00 UTC
Updated	2023-11-07 03:50:00 UTC
Description	An issue was discovered in net/netfilter/nf_tables_api.c in the Linux kernel before 5.19.6. A denial of service can occur upon

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link	Tags
[PATCH net 11/14] netfilter: nf_tables: disallow binding to already bound chain - Pablo Neira Ayuso		lore.kernel.org	
JavaScript is not available.	MISC	twitter.com	
[SECURITY] [DLA 3173-1] linux-5.10 security update	MLIST	lists.debian.org	
[PATCH net 11/14] netfilter: nf_tables: disallow binding to already bound chain - Pablo Neira Ayuso	MISC	lore.kernel.org	
netfilter: nf_tables: disallow binding to already bound chain · torvalds/linux@e02f0d3 · GitHub	MISC	github.com	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.6	MISC	cdn.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160270 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-8267)

181018 Debian Security Update for linux (CVE-2022-39190)

181190 Debian Security Update for linux-5.10 (DLA 3173-1)

199031 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5729-1)

199038 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5729-2)

240869 Red Hat Update for kernel-rt (RHSA-2022:7933)

240904 Red Hat Update for kernel security (RHSA-2022:8267)

354082 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-008

354084 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-020

354439 Amazon Linux Security Advisory for kernel : ALAS2022-2022-150

354468 Amazon Linux Security Advisory for kernel : ALAS2022-2022-185

354542 Amazon Linux Security Advisory for kernel : ALAS-2022-185

355199 Amazon Linux Security Advisory for kernel : ALAS2023-2023-070

377891 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0002)

378468 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-20230042)

378512 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0042)

6140091 AWS Bottlerocket Security Update for kernel (GHSA-w2pg-2x8r-7ff5)

672495 EulerOS Security Update for kernel (EulerOS-SA-2023-1012)

672516 EulerOS Security Update for kernel (EulerOS-SA-2023-1037)

752589 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3264-1)

752594 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3293-1)

753063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:4617-1)

753167 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3288-1)

753370 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3609-1)

753374 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3809-1)

903741 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10877)

903823 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10860)

904094 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10877-1)

904141 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10860-1)

904141 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10860-1)

906055 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10877-2)

906298 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (10860-2)

940798 AlmaLinux Security Update for kernel (ALSA-2022:8267)

940843 AlmaLinux Security Update for kernel-rt (ALSA-2022:7933)