CVE-2022-32250

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-32250
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-02 21:15:00 UTC
Updated	2023-11-07 03:47:00 UTC
Description	net/netfilter/nf_tables_api.c in the Linux kernel through 5.18.1 allows a local user (able to create user/net namespaces) to e

Risk And Classification

Problem Types: CWE-416

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	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference
oss-security - Re: Linux kernel: Netfilter heap buffer overflow: Is this CVE-2022-32250?
oss-security - Linux kernel: Netfilter heap buffer overflow: Is this CVE-2022-32250?
oss-security - Re: Linux Kernel use-after-free write in netfilter
kernel/git/netdev/net.git - Netdev Group's networking tree
CVE-2022-32250 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security
Debian -- Security Information -- DSA-5173-1 linux
Debian -- Security Information -- DSA-5161-1 linux
[SECURITY] Fedora 36 Update: kernel-5.17.13-300.fc36 - package-announce - Fedora Mailing-Lists
oss-security - Re: Linux Kernel use-after-free write in netfilter
oss-security - Linux Kernel use-after-free write in netfilter
oss-security - Re: Linux Kernel use-after-free write in netfilter
[SECURITY] [DLA 3065-1] linux security update
oss-security - Re: Linux Kernel use-after-free write in netfilter
2092427 – (CVE-2022-1966) CVE-2022-1966 kernel: a use-after-free write in the netfilter subsystem can lead to privilege escalation to root
[SECURITY] Fedora 36 Update: kernel-5.17.13-300.fc36 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 35 Update: kernel-5.17.13-200.fc35 - package-announce - Fedora Mailing-Lists
Linux Kernel Exploit (CVE-2022-32250) with mqueue | Theori
[SECURITY] Fedora 35 Update: kernel-5.17.13-200.fc35 - package-announce - Fedora Mailing-Lists
oss-security - Re: Linux Kernel use-after-free write in netfilter
GitHub - theori-io/CVE-2022-32250-exploit
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

160012 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9667)

160028 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-5819)

180282 Debian Security Update for linux (DLA 3065-1)

180605 Debian Security Update for linux (DSA 5173-1)

183416 Debian Security Update for linux (CVE-2022-32250)

240544 Red Hat Update for kernel-rt (RHSA-2022:5633)

240545 Red Hat Update for kernel (RHSA-2022:5626)

240550 Red Hat Update for kpatch-patch (RHSA-2022:5641)

240581 Red Hat Update for kernel-rt (RHSA-2022:5834)

240584 Red Hat Update for kpatch-patch (RHSA-2022:5839)

240594 Red Hat Update for kernel (RHSA-2022:5819)

257172 CentOS Security Update for kernel (CESA-2022:5232)

353976 Amazon Linux Security Advisory for kernel : ALAS-2022-1604

353985 Amazon Linux Security Advisory for kernel : ALAS2-2022-1813

353993 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-016

353994 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-028

354007 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-015

354008 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-030

354017 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-032

354018 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-003

354022 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-002

354023 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-017

354024 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-004

354270 Amazon Linux Security Advisory for kernel : ALAS2022-2022-114

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

377026 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0035)

377110 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0146)

377117 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)

377871 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0001)

390264 Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0021)

6140393 AWS Bottlerocket Security Update for kernel (GHSA-mjp2-3qxw-rgg7)

672017 EulerOS Security Update for kernel (EulerOS-SA-2022-2244)

672045 EulerOS Security Update for kernel (EulerOS-SA-2022-2225)

672086 EulerOS Security Update for kernel (EulerOS-SA-2022-2321)

672139 EulerOS Security Update for kernel (EulerOS-SA-2022-2428)

752502 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2875-1)

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

752632 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:3450-1)

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

753091 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2172-1)

753135 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2722-1)

753153 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 13 for SLE 15 SP3) (SUSE-SU-2022:2239-1)

753156 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2741-1)

753169 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 26 for SLE 15 SP2) (SUSE-SU-2022:2230-1)

753243 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP3) (SUSE-SU-2022:2216-1)

753253 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 15 for SLE 15 SP3) (SUSE-SU-2022:2245-1)

753296 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2177-1)

753330 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP4) (SUSE-SU-2022:2268-1)

753353 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 17 for SLE 15 SP3) (SUSE-SU-2022:2262-1)

753486 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 19 for SLE 15 SP3) (SUSE-SU-2022:2214-1)

902155 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9873)

902158 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9879)

902277 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9879-1)

902483 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9873-1)

906019 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9873-2)

906353 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9879-2)

940602 AlmaLinux Security Update for kernel-rt (ALSA-2022:5834)

940612 AlmaLinux Security Update for kernel (ALSA-2022:5819)

960162 Rocky Linux Security Update for kernel-rt (RLSA-2022:5834)

960164 Rocky Linux Security Update for kernel (RLSA-2022:5819)