CVE-2021-3483

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3483
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-17 12:15:00 UTC
Updated	2022-05-13 19:40:00 UTC
Description	A flaw was found in the Nosy driver in the Linux kernel. This issue allows a device to be inserted twice into a doubly-linked l

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	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.12	-	All	All
Operating System	Linux	Linux Kernel	5.12	rc1	All	All
Operating System	Linux	Linux Kernel	5.12	rc2	All	All
Operating System	Linux	Linux Kernel	5.12	rc3	All	All
Operating System	Linux	Linux Kernel	5.12	rc4	All	All
Operating System	Linux	Linux Kernel	5.12	rc5	All	All
Application	Netapp	Cloud Backup	-	All	All	All
Hardware	Netapp	H300e	-	All	All	All
Operating System	Netapp	H300e Firmware	-	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	H500e	-	All	All	All
Operating System	Netapp	H500e Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All

References

Reference
1948045 – (CVE-2021-3483) CVE-2021-3483 kernel: use-after-free in nosy driver in nosy_ioctl() in drivers/firewire/nosy.c when a device is ad
[SECURITY] [DLA 2689-1] linux security update
oss-security - CVE-2021-3483: Linux kernel: a use-after-free bug in nosy driver
[SECURITY] [DLA 2690-1] linux-4.19 security update
CVE-2021-3483 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 174916 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1210-1)
- 174917 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1211-1)
- 174919 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1238-1)
- 174925 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1248-1)
- 174938 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1301-1)
- 174996 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:14724-1)
- 178679 Debian Security Update for linux-4.19 (DLA 2690-1)
- 178680 Debian Security Update for linux (DLA 2689-1)
- 179529 Debian Security Update for linux (CVE-2021-3483)
- 198365 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4948-1)
- 198398 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4979-1)

198401 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4982-1)

198403 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4984-1)

352274 Amazon Linux Security Advisory for kernel: ALAS2-2021-1627

670416 EulerOS Security Update for kernel (EulerOS-SA-2021-1983)

670438 EulerOS Security Update for kernel (EulerOS-SA-2021-2062)

670449 EulerOS Security Update for kernel (EulerOS-SA-2021-2051)

670463 EulerOS Security Update for kernel (EulerOS-SA-2021-2221)

670634 EulerOS Security Update for kernel (EulerOS-SA-2021-2392)

671047 EulerOS Security Update for kernel (EulerOS-SA-2021-2588)

750004 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)

750006 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)

750014 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1623-1)

750015 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1624-1)

750199 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)

750261 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0579-1)

750650 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)

750652 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)

750762 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)

750766 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)

900096 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

901455 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6568-1)

903117 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4234)

905927 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4234-1)

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.

CVE.report and Source URL Uptime Status status.cve.report