CVE-2021-3772

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3772
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-02 23:15:00 UTC
Updated	2023-02-12 23:42:00 UTC
Description	A flaw was found in the Linux SCTP stack. A blind attacker may be able to kill an existing SCTP association through invalid

Risk And Classification

Problem Types: CWE-354

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	Linux	Linux Kernel	All	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.0	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.0.0	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.20	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.25	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.30	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.30.5r3	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.40	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.40.3r2	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.40.5	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.50.1	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.50.2	-	All	All
Application	Netapp	E-series Santricity Os Controller	11.50.2	p1	All	All
Application	Netapp	E-series Santricity Os Controller	11.60	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.60.0	All	All	All

Application	Netapp	E-series Santricity Os Controller	11.60.1	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.60.3	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.70.1	All	All	All
Application	Netapp	E-series Santricity Os Controller	11.70.2	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	H610c	-	All	All	All
Operating System	Netapp	H610c Firmware	-	All	All	All
Hardware	Netapp	H610s	-	All	All	All
Operating System	Netapp	H610s Firmware	-	All	All	All
Hardware	Netapp	H615c	-	All	All	All
Operating System	Netapp	H615c Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Netapp	Solidfire Hci Storage Node	-	All	All	All
Application	Oracle	Communications Cloud Native Core Binding Support Function	22.1.3	All	All	All
Application	Oracle	Communications Cloud Native Core Network Exposure Function	22.1.1	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	22.2.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source
Merge branch 'sctp-enhancements-for-the-verification-tag' · torvalds/linux@32f8807 · GitHub	MISC
CVE-2021-3772 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM
[SECURITY] [DLA 2941-1] linux-4.19 security update	MLIST
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC

CVE-2021-3772 | Ubuntu	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
2000694 – (CVE-2021-3772) CVE-2021-3772 kernel: sctp: Invalid chunks may be used to remotely remove existing associations	MISC
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC
Debian -- Security Information -- DSA-5096-1 linux	DEBIAN
Oracle Critical Patch Update Advisory - July 2022	N/A
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159741 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9260)
- 159825 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-1988)
- 179117 Debian Security Update for linux (DSA 5096-1)
- 179119 Debian Security Update for linux-4.19 (DLA 2941-1)
- 180413 Debian Security Update for linux (CVE-2021-3772)
- 198589 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5165-1)
- 198653 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5265-1)
- 198824 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5467-1)
- 198825 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5466-1)
- 199560 Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6001-1)
- 199568 Ubuntu Security Notification for Linux kernel (AWS) Vulnerabilities (USN-6013-1)
- 199577 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6014-1)
- 240275 Red Hat Update for kernel-rt (RHSA-2022:1975)
- 240298 Red Hat Update for kernel security (RHSA-2022:1988)
- 282164 Fedora Security Update for kernel (FEDORA-2021-a093973910)
- 353079 Amazon Linux Security Advisory for kernel : ALAS2-2021-1727
- 353141 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-010
- 353152 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-008
- 353161 Amazon Linux Security Advisory for kernel : ALAS-2022-1563

353242 Amazon Linux Security Advisory for kernel : ALAC2012-2022-036

353243 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-037

353244 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-038

354747 Amazon Linux Security Advisory for kernel : ALAS-2023-1688

390258 Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0011)

671344 EulerOS Security Update for kernel (EulerOS-SA-2022-1271)

671436 EulerOS Security Update for kernel (EulerOS-SA-2022-1352)

671630 EulerOS Security Update for kernel (EulerOS-SA-2022-1647)

671631 EulerOS Security Update for kernel (EulerOS-SA-2022-1661)

671703 EulerOS Security Update for kernel (EulerOS-SA-2022-1735)

671723 EulerOS Security Update for kernel (EulerOS-SA-2022-1780)

671724 EulerOS Security Update for kernel (EulerOS-SA-2022-1779)

751336 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1460-1)

751342 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3641-1)

751346 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3655-1)

751349 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1477-1)

751353 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3675-1)

751424 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3848-1)

751437 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3876-1)

751441 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3876-1)

751451 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)

751473 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3969-1)

751476 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3972-1)

900733 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8879)

901317 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8879-1)

905899 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8879-2)

940517 AlmaLinux Security Update for kernel (ALSA-2022:1988)

960132 Rocky Linux Security Update for kernel-rt (RLSA-2022:1975)

960134 Rocky Linux Security Update for kernel (RLSA-2022:1988)