CVE-2021-23133

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-23133
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-04-22 18:15:00 UTC
Updated	2023-11-07 03:30:00 UTC
Description	A race condition in Linux kernel SCTP sockets (net/sctp/socket.c) before 5.12-rc8 can lead to kernel privilege escalation fro

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Broadcom	Brocade Fabric Operating System	-	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	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
Operating System	Linux	Linux Kernel	5.12	rc6	All	All
Operating System	Linux	Linux Kernel	5.12	rc7	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
Hardware	Netapp	Solidfire Baseboard Management Controller	-	All	All	All
Operating System	Netapp	Solidfire Baseboard Management Controller Firmware	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All

References

Reference	Source	Link	T
[SECURITY] Fedora 33 Update: kernel-5.11.16-200.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 34 Update: kernel-5.11.16-300.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 34 Update: kernel-5.11.16-300.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] [DLA 2689-1] linux security update	MLIST	lists.debian.org	
[SECURITY] Fedora 33 Update: kernel-5.11.16-200.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 32 Update: kernel-5.11.16-100.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] [DLA 2690-1] linux-4.19 security update	MLIST	lists.debian.org	
CVE-2021-23133 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
oss-security - Re: CVE-2021-23133: Linux kernel: race condition in sctp sockets	MLIST	www.openwall.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	
oss-security - Re: CVE-2021-23133: Linux kernel: race condition in sctp sockets	MLIST	www.openwall.com	
[SECURITY] Fedora 32 Update: kernel-5.11.16-100.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
oss-security - Re: CVE-2021-23133: Linux kernel: race condition in sctp sockets	MLIST	www.openwall.com	
oss-security - CVE-2021-23133: Linux kernel: race condition in sctp sockets	CONFIRM	www.openwall.com	
oss-security - Re: CVE-2021-23133: Linux kernel: race condition in sctp sockets	MLIST	www.openwall.com	

CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

Vendor Comments And Credit

Discovery Credit

LEGACY: Or Cohen from Palo Alto Networks

Legacy QID Mappings

- 159277 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9306)
- 159278 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9307)
- 159304 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9349)
- 159305 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9351)
- 159306 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9362)
- 159307 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9363)
- 159492 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)
- 178679 Debian Security Update for linux-4.19 (DLA 2690-1)
- 178680 Debian Security Update for linux (DLA 2689-1)
- 179939 Debian Security Update for linux (CVE-2021-23133)
- 198416 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4997-1)
- 198417 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4999-1)
- 198418 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-5000-1)
- 198419 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-5001-1)
- 198421 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-5003-1)
- 198425 Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-5000-2)
- 198426 Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-4997-2)
- 239816 Red Hat Update for kernel security (RHSA-2021:4356)
- 239879 Red Hat Update for kernel-rt (RHSA-2021:4140)
- 281274 Fedora Security Update for kernel (FEDORA-2021-a963f04012)
- 281275 Fedora Security Update for kernel (FEDORA-2021-e6b4847979)
- 281276 Fedora Security Update for kernel (FEDORA-2021-8cd093f639)

352366 Amazon Linux Security Advisory for kernel: ALAS-2021-1503

352375 Amazon Linux Security Advisory for kernel: ALAS2-2021-1636

353148 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-003

353159 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-001

376371 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Linux kernel Vulnerability (K67416037)

6140265 AWS Bottlerocket Security Update for kernel (GHSA-x849-g985-wxr9)

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)

750117 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1891-1)

750125 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1887-1)

750139 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1913-1)

750140 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1912-1)

750864 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2421-1)

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

901089 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6530-1)

902857 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4156)

905762 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4156-1)

940265 AlmaLinux Security Update for kernel (ALSA-2021:4356)