



# CVE-2023-28466

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-28466
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-03-16 00:15:00 UTC
<b>Updated</b>	2023-11-09 13:57:00 UTC
<b>Description</b>	do_tls_getsockopt in net/tls/tls_main.c in the Linux kernel through 6.2.6 lacks a lock_sock call, leading to a race condition (v

## Risk And Classification

**Problem Types:** CWE-476

## 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
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	Baseboard Management Controller H300s	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410c	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410s	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500s	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H700s	-	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All

## References

Reference	Source	Link	Tags
-----------	--------	------	------

[SECURITY] [DLA 3404-1] linux-5.10 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	
CVE-2023-28466 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, ar

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [160800](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-3847)
- [160806](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2023-3723)
- [181765](#) Debian Security Update for linux-5.10 (DLA 3404-1)
- [184979](#) Debian Security Update for linux (CVE-2023-28466)
- [199298](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6033-1)
- [199422](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6175-1)
- [199437](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6186-1)
- [199650](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6284-1)
- [199669](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6301-1)
- [199670](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6300-1)
- [199764](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6385-1)
- [241733](#) Red Hat Update for kernel (RHSA-2023:3723)
- [241740](#) Red Hat Update for kernel-rt (RHSA-2023:3708)
- [241751](#) Red Hat Update for kernel-rt (RHSA-2023:3819)
- [241752](#) Red Hat Update for kernel security (RHSA-2023:3847)
- [354882](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-121
- [354883](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-016
- [354885](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-029
- [354886](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-119
- [354887](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-120
- [354888](#) Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-118

<a href="#">354904</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-044
<a href="#">355178</a> Amazon Linux Security Advisory for kernel : ALAS2023-2023-148
<a href="#">355185</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-002
<a href="#">355228</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2023LIVEPATCH-2023-003
<a href="#">355526</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-130
<a href="#">355528</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-129
<a href="#">355529</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-132
<a href="#">355530</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-133
<a href="#">355533</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-128
<a href="#">355535</a> Amazon Linux Security Advisory for kernel-livepatch : ALAS2LIVEPATCH-2023-131
<a href="#">355545</a> Amazon Linux Security Advisory for kernel : ALAS2-2023-2100
<a href="#">355557</a> Amazon Linux Security Advisory for kernel : ALAS-2023-1773
<a href="#">378537</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0048)
<a href="#">378710</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2023:0079)
<a href="#">6140104</a> AWS Bottlerocket Security Update for kernel (GHSA-9fh9-wqhq-6x64)
<a href="#">672935</a> EulerOS Security Update for kernel (EulerOS-SA-2023-1824)
<a href="#">672952</a> EulerOS Security Update for kernel (EulerOS-SA-2023-1806)
<a href="#">673005</a> EulerOS Security Update for kernel (EulerOS-SA-2023-1873)
<a href="#">673074</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2193)
<a href="#">673182</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2335)
<a href="#">673393</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2647)
<a href="#">674113</a> EulerOS Security Update for kernel (EulerOS-SA-2023-2689)
<a href="#">753902</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:1800-1)
<a href="#">753905</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:1811-1)
<a href="#">754097</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2507-1)
<a href="#">754106</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2534-1)
<a href="#">754110</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:2538-1)
<a href="#">906809</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (25651-1)
<a href="#">906863</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (25661-1)

941166 AlmaLinux Security Update for kernel (ALSA-2023:3723)

941167 AlmaLinux Security Update for kernel-rt (ALSA-2023:3708)

941193 AlmaLinux Security Update for kernel (ALSA-2023:3847)

941194 AlmaLinux Security Update for kernel-rt (ALSA-2023:3819)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)**