CVE-2020-36385

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-36385
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-07 12:15:00 UTC
Updated	2022-10-25 16:42:00 UTC
Description	An issue was discovered in the Linux kernel before 5.10. drivers/infiniband/core/ucma.c has a use-after-free because the ct

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	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

Application	Starwindsoftware	Starwind San Nas	v8r12	All	All	All
Application	Starwindsoftware	Starwind Virtual San	v8	build14338	All	All

References

Reference	Source	Link	Tags
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
KASAN: use-after-free Read in ucma_close (2)	MISC	syzkaller.appspot.com	
SyzScope - KASAN: use-after-free Read in ucma_close (2)	MISC	sites.google.com	
CVE-2020-36385 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
CVE-2020-36385 Linux kernel vulnerability in StarWind products	MISC	www.starwindsoftware.com	
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.10	MISC	cdn.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- 159443 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4056)
- 159538 Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4777)
- 160101 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-9793)
- 198562 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5136-1)
- 198563 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5137-1)
- 198565 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5137-2)
- 239762 Red Hat Update for kernel-rt (RHSA-2021:4088)
- 239771 Red Hat Update for kernel security (RHSA-2021:4056)
- 239772 Red Hat Update for kpatch-patch (RHSA-2021:4122)
- 239852 Red Hat Update for kpatch-patch (RHSA-2021:4597)
- 239894 Red Hat Update for kernel (RHSA-2021:4687)
- 239902 Red Hat Update for kernel (RHSA-2021:4777)
- 239904 Red Hat Update for kernel-rt (RHSA-2021:4779)
- 239906 Red Hat Update for kpatch-patch (RHSA-2021:4798)
- 239914 Red Hat Update for kpatch-patch (RHSA-2021:4859)

239917 Red Hat Update for kernel (RHSA-2021:4871)

239918 Red Hat Update for kernel-rt (RHSA-2021:4875)

257131 CentOS Security Update for kernel (CESA-2021:4777)

670707 EulerOS Security Update for kernel (EulerOS-SA-2021-2465)

670744 EulerOS Security Update for kernel (EulerOS-SA-2021-2502)

670772 EulerOS Security Update for kernel (EulerOS-SA-2021-2530)

670796 EulerOS Security Update for kernel (EulerOS-SA-2021-2554)

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

750748 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2202-1)

750750 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2184-1)

750844 SUSE Enterprise Linux Security Update for kernel (SUSE-SU-2021:2407-1)

750848 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2416-1)(Sequoia)

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

750868 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2427-1)

750869 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2422-1)

750877 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2427-1)

750880 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2451-1)

750899 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 36 for SLE 12 SP3) (SUSE-SU-2021:2538-1)

940068 AlmaLinux Security Update for kernel (ALSA-2021:4056)

960019 Rocky Linux Security Update for kernel-rt (RLSA-2021:4088)

960061 Rocky Linux Security Update for kernel (RLSA-2021:4056)

© 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 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