CVE-2023-5178

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-5178
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-01 17:15:00 UTC
Updated	2024-04-03 14:15:00 UTC
Description	A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the N

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
Operating System	Linux	Linux Kernel	6.6	rc1	All	All
Operating System	Linux	Linux Kernel	6.6	rc2	All	All
Operating System	Linux	Linux Kernel	6.6	rc3	All	All
Operating System	Linux	Linux Kernel	6.6	rc4	All	All
Operating System	Linux	Linux Kernel	6.6	rc5	All	All
Operating System	Linux	Linux Kernel	6.6	rc6	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All
Application	Netapp	Solidfire Hci Storage Node	-	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All

References

Reference	Source	Link
RHSA-2023:7557		access.redhat.com
Red Hat		access.redhat.com

Red Hat		access.redhat.com
RHSA-2024:1278		access.redhat.com
2241924 – (CVE-2023-5178) CVE-2023-5178 kernel: use after free in nvmet_tcp_free_crypto in NVMe	MISC	bugzilla.redhat.com
RHSA-2023:7551		access.redhat.com
RHSA-2024:1269		access.redhat.com
CVE-2023-5178 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security		security.netapp.com
Red Hat		access.redhat.com
[PATCH] nvmet-tcp: Fix a possible UAF in queue intialization setup - Sagi Grimberg	MISC	lore.kernel.org
RHSA-2023:7549		access.redhat.com
RHSA-2023:7554		access.redhat.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
RHSA-2024:1268		access.redhat.com
Red Hat		access.redhat.com
Red Hat		access.redhat.com
cve-details	MISC	access.redhat.com
RHSA-2023:7559		access.redhat.com
RHSA-2023:7548		access.redhat.com
Red Hat		access.redhat.com
[SECURITY] [DLA 3711-1] linux-5.10 security update		lists.debian.org
Red Hat		access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

161208 Oracle Enterprise Linux Security Update for kernel (ELSA-2023-7549)

161229 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-13044)

161237 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2023-13043)

161238 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-13049)

161239 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2023-13048)

161318 Oracle Enterprise Linux Security Update for kernel (ELSA-2024-12094)

161404 Oracle Enterprise Linux Security Update for kernel (ELSA-2024-0461)

199929 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-6497-1)

199976 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6534-1)

199980 Ubuntu Security Notification for Linux kernel Vulnerability (USN-6536-1)

199982 Ubuntu Security Notification for Linux kernel (GCP) Vulnerability (USN-6537-1)

199996 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6549-1)

199997 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6548-1)

199999 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6548-2)

200002 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6534-2)

200003 Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-6549-2)

200006 Ubuntu Security Notification for Linux kernel (Oracle) Vulnerabilities (USN-6548-3)

200007 Ubuntu Security Notification for Linux kernel (Low Latency) Vulnerabilities (USN-6549-3)

200010 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6534-3)

200024 Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6549-4)

200035 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6549-5)

200037 Ubuntu Security Notification for Linux kernel (IoT) Vulnerabilities (USN-6548-5)

200113 Ubuntu Security Notification for Linux kernel (GCP) Vulnerabilities (USN-6635-1)

242482 Red Hat Update for kernel-rt (RHSA-2023:7379)

242497 Red Hat Update for kpatch-patch (RHSA-2023:7418)

242515 Red Hat Update for kernel (RHSA-2023:7557)

242516 Red Hat Update for kernel (RHSA-2023:7549)

242522 Red Hat Update for kpatch-patch (RHSA-2023:7554)

242526 Red Hat Update for kernel-rt (RHSA-2023:7548)

242528 Red Hat Update for kernel-rt (RHSA-2023:7551)

242529 Red Hat Update for kpatch-patch (RHSA-2023:7559)

242612 Red Hat Update for kernel security (RHSA-2023:7370)

242727 Red Hat Update for kpatch-patch (RHSA-2024:0340)

242728 Red Hat Update for kpatch-patch (RHSA-2024:0378)

242738 Red Hat Update for kpatch-patch (RHSA-2024:0386)

242759 Red Hat Update for kernel (RHSA-2024:0432)

242769 Red Hat Update for kpatch-patch (RHSA-2024:0554)

242789 Red Hat Update for kernel (RHSA-2024:0575)

242839 Red Hat Update for kernel (RHSA-2024:0461)

242847 Red Hat Update for kernel-rt (RHSA-2024:0431)

242855 Red Hat Update for kernel (RHSA-2024:0412)

243055 Red Hat Update for kernel (RHSA-2024:1268)

243057 Red Hat Update for kpatch-patch (RHSA-2024:1278)

243058 Red Hat Update for kernel-rt (RHSA-2024:1269)

356572 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2023-040

379614 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2024:0017)

6000419 Debian Security Update for linux (DSA 5594-1)

6000428 Debian Security Update for linux-5.10 (DLA 3711-1)

673595 EulerOS Security Update for kernel (EulerOS-SA-2023-3247)

673692 EulerOS Security Update for kernel (EulerOS-SA-2023-3275)

673714 EulerOS Security Update for kernel (EulerOS-SA-2024-1196)

755238 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4378-1)

755240 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4375-1)

755249 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4414-1)

755563 SUSE Security Update for the linux kernel (SUSE-SU-2023:4351-1)

755566 SUSE Security Update for the linux kernel (SUSE-SU-2023:4345-1)

755567 SUSE Security Update for the linux kernel (SUSE-SU-2023:4343-1)

755706 SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 3 for SLE 15 SP4) (SUSE-SU-2024:0331-1)

755709 SUSE Enterprise Linux Security Update for the Linux Kernel RT (Live Patch 5 for SLE 15 SP5) (SUSE-SU-2024:0348-1)

755714 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 3 for SLE 15 SP5) (SUSE-SU-2024:0352-1)

755715 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 5 for SLE 15 SP5) (SUSE-SU-2024:0378-1)

755718 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 6 for SLE 15 SP5) (SUSE-SU-2024:0395-1)

755726 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 8 for SLE 15 SP4) (SUSE-SU-2024:0414-1)

755728 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 7 for SLE 15 SP4) (SUSE-SU-2024:0421-1)

907626 Common Base Linux Mariner (CBL-Mariner) Security Update for hyperv-daemons (31777-1)

907632 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (31852)

907677 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (31852-1)

941482 AlmaLinux Security Update for kernel (ALSA-2023:7549)

961087 Rocky Linux Security Update for kernel-rt (RLSA-2023:7548)

961089 Rocky Linux Security Update for kernel (RLSA-2023:7549)