CVE-2022-1055

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-1055
State	PUBLIC
Assigner	security@google.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-29 15:15:00 UTC
Updated	2022-10-19 17:40:00 UTC
Description	A use-after-free exists in the Linux Kernel in tc_new_tfilter that could allow a local attacker to gain privilege escalation. The

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Canonical	Ubuntu Linux	21.10	All	All	All
Operating System	Canonical	Ubuntu Linux	22.04	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.17	-	All	All
Operating System	Linux	Linux Kernel	5.17	rc1	All	All
Operating System	Linux	Linux Kernel	5.17	rc2	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
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link	Tags
CVE-2022-1055 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	
KASAN: use-after-free Write in mini_qdisc_pair_swap (2)	CONFIRM	syzkaller.appspot.com	
Kernel Live Patch Security Notice LSN-0086-1 ≈ Packet Storm	MISC	packetstormsecurity.com	
????????	CONFIRM	kernel.dance	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159785 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel-container (ELSA-2022-9368)

159788 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9365)

160039 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-6003)

160210 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-7683)

179206 Debian Security Update for linux (CVE-2022-1055)

198721 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5358-1)

198727 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5358-2)

198731 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5368-1)

198740 Ubuntu Security Notification for Linux kernel (BlueField) Vulnerabilities (USN-5377-1)

240600 Red Hat Update for kernel-rt (RHSA-2022:6002)

240604 Red Hat Update for kernel security (RHSA-2022:6003)

240815 Red Hat Update for kernel-rt (RHSA-2022:7444)

240817 Red Hat Update for kernel security (RHSA-2022:7683)

243041 Red Hat Update for kernel security (RHSA-2024:1188)

354279 Amazon Linux Security Advisory for kernel : ALAS2022-2022-039

354468 Amazon Linux Security Advisory for kernel : ALAS2022-2022-185

354542 Amazon Linux Security Advisory for kernel : ALAS-2022-185

355199 Amazon Linux Security Advisory for kernel : ALAS2023-2023-070

376925 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)

610430 Google Android September 2022 Security Patch Missing for Huawei EMUI

610432 Google Pixel Android August 2022 Security Patch Missing

671817 EulerOS Security Update for kernel (EulerOS-SA-2022-1868)

672003 EulerOS Security Update for kernel (EulerOS-SA-2022-2134)

752036 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1183-1)

752042 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1197-1)

753137 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 15 for SLE 15 SP3) (SUSE-SU-2022:1453-1)

753373 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1257-1)

753390 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 14 for SLE 15 SP3) (SUSE-SU-2022:1326-1)

753417 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1163-1)

753427 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1407-1)

753445 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 12 for SLE 15 SP3) (SUSE-SU-2022:1369-1)

900793 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9217)

901319 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9217-1)

901965 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9218-1)

906042 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9217-2)

906430 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9218-2)

940634 AlmaLinux Security Update for kernel (ALSA-2022:6003)

940637 AlmaLinux Security Update for kernel-rt (ALSA-2022:6002)

940732 AlmaLinux Security Update for kernel (ALSA-2022:7683)

940766 AlmaLinux Security Update for kernel-rt (ALSA-2022:7444)

960176 Rocky Linux Security Update for kernel-rt (RLSA-2022:7444)

960184 Rocky Linux Security Update for kernel (RLSA-2022:7683)