CVE-2021-3753

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3753
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-16 19:15:00 UTC
Updated	2022-12-07 01:58:00 UTC
Description	A race problem was seen in the vt_k_ioctl in drivers/tty/vt/vt_ioctl.c in the Linux kernel, which may cause an out of bounds r

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All
Operating System	Netapp	Bootstrap Os	-	All	All	All
Application	Netapp	Element Software	-	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	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Hardware	Netapp	Hci Compute Node	-	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All

Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All

References

Reference	Source	Link
CVE-2021-3753 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com
oss-security - CVE-2021-3753: A out-of-bounds caused by the race of KDSETMODE in vt for latest Linux	MISC	www.openwall.com
1999589 – (CVE-2021-3753) CVE-2021-3753 kernel: a race out-of-bound read in vt	MISC	bugzilla.redhat.com
vt_kdsetmode: extend console locking · torvalds/linux@2287a51 · GitHub	MISC	github.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

- 159621 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2022-9088)
- 178809 Debian Security Update for linux (DSA 4978-1)
- 178844 Debian Security Update for linux-4.19 (DLA 2785-1)
- 178943 Debian Security Update for linux (DLA 2843-1)
- 179563 Debian Security Update for linux (CVE-2021-3753)
- 198540 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5113-1)
- 198542 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5115-1)
- 198543 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5117-1)
- 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)
- 199522 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6221-1)
- 352839 Amazon Linux Security Advisory for kernel: ALAS2-2021-1704
- 352871 Amazon Linux Security Advisory for kernel : ALAS-2021-1539
- 353144 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-007
- 353155 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-005

353242 Amazon Linux Security Advisory for kernel : ALAC2012-2022-036

353243 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-037

353244 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-038

356186 Amazon Linux Security Advisory for microvm-kernel : ALASMICROVM-KERNEL-4.14-2023-003

356218 Amazon Linux Security Advisory for microvm-kernel : ALASMICROVM-KERNEL-4.14-2023-002

390256 Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2022-0007)

610418 Google Pixel Android June 2022 Security Patch Missing

610422 Google Android July 2022 Security Patch Missing for Huawei EMUI

6140330 AWS Bottlerocket Security Update for kernel (GHSA-fj39-g84c-hc66)

671134 EulerOS Security Update for kernel (EulerOS-SA-2021-2688)

671135 EulerOS Security Update for kernel (EulerOS-SA-2021-2636)

671181 EulerOS Security Update for kernel (EulerOS-SA-2021-2934)

671219 EulerOS Security Update for kernel (EulerOS-SA-2022-1030)

671252 EulerOS Security Update for kernel (EulerOS-SA-2022-1171)

751137 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1271-1)

751155 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3192-1)

751160 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3179-1)

751163 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3206-1)

751170 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3205-1)

751437 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3876-1)

751441 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3876-1)

751451 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)

751473 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3969-1)

751476 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3972-1)

753441 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:14905-1)

900721 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8675)

906132 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8675-1)

CVE.report and Source URL Uptime Status status.cve.report