



CVE-2020-25668

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-25668
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-26 12:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	A flaw was found in Linux Kernel because access to the global variable fg_console is not properly synchronized leading to a

Risk And Classification

Problem Types: CWE-662

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	5.9.2	All	All	All
Hardware	Netapp	500f	-	All	All	All
Operating System	Netapp	500f Firmware	-	All	All	All
Hardware	Netapp	A250	-	All	All	All
Operating System	Netapp	A250 Firmware	-	All	All	All
Application	Netapp	Cloud Backup	-	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
Hardware	Netapp	Solidfire Baseboard Management Controller	-	All	All	All
Operating System	Netapp	Solidfire Baseboard Management Controller Firmware	-	All	All	All
Application	Netapp	Solidfire Hci Management Node	-	All	All	All

References

Reference	Source	Link	Tags
Invalid Bug ID	MISC	bugzilla.redhat.com	
CVE-2020-25668 Linux Kernel Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com	
oss-security - Re: CVE-2020-25668: Linux kernel concurrency use-after-free in vt	MLIST	www.openwall.com	
[SECURITY] [DLA 2494-1] linux security update	MLIST	lists.debian.org	
oss-security - Re: CVE-2020-25668: Linux kernel concurrency use-after-free in vt		www.openwall.com	
oss-security - CVE-2020-25668: Linux kernel concurrency use-after-free in vt		www.openwall.com	
oss-security - CVE-2020-25668: Linux kernel concurrency use-after-free in vt	MLIST	www.openwall.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	
oss-security - CVE-2020-25668: Linux kernel concurrency use-after-free in vt	MISC	www.openwall.com	
oss-security - Re: CVE-2020-25668: Linux kernel concurrency use-after-free in vt	MISC	www.openwall.com	
Invalid Bug ID		bugzilla.redhat.com	
[SECURITY] [DLA 2483-1] linux-4.19 security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[353100](#) Amazon Linux Security Advisory for kernel : ALAC2012-2021-024

[353101](#) Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025

[353102](#) Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026

[353133](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-018

[377038](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)

[390217](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for Unbreakable Enterprise kernel (OVMSA-2021-0001)

[610384](#) Google Pixel Android December 2021 Security Patch Missing

[610392](#) Google Android January 2022 Security Patch Missing for Huawei EMUI

[6140361](#) AWS Bottlerocket Security Update for kernel (GHSA-m78q-4mgc-289q)

[750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)

[750488](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2260-1)

[750533](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2112-1)

[750609](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:1906-1)

© [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](#)