



# CVE-2020-29660

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-29660
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-12-09 17:15:00 UTC
<b>Updated</b>	2023-11-07 03:21:00 UTC
<b>Description</b>	A locking inconsistency issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_io.c and

## Risk And Classification

**Problem Types:** CWE-416 | CWE-667

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Broadcom	Fabric Operating System	-	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Hardware	Netapp	8300	-	All	All	All
Operating System	Netapp	8300 Firmware	-	All	All	All
Hardware	Netapp	8700	-	All	All	All
Operating System	Netapp	8700 Firmware	-	All	All	All
Hardware	Netapp	A400	-	All	All	All
Operating System	Netapp	A400 Firmware	-	All	All	All
Hardware	Netapp	A700s	-	All	All	All
Operating System	Netapp	A700s Firmware	-	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	All	All

Hardware	<a href="#">Netapp</a>	<a href="#">H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Solidfire Baseboard Management Controller</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Solidfire Baseboard Management Controller Firmware</a>	-	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 32 Update: kernel-5.9.14-100.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] [DLA 2557-1] linux-4.19 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
[SECURITY] [DLA 2586-1] linux security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Kernel Live Patch Security Notice LSN-0082-1 ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>
[SECURITY] Fedora 32 Update: kernel-5.9.14-100.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
oss-security - 2 kernel issues	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
Debian -- Security Information -- DSA-4843-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
December 2020 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>
[SECURITY] Fedora 33 Update: kernel-5.9.14-200.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 33 Update: kernel-5.9.14-200.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">159492</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)
<a href="#">239816</a> Red Hat Update for kernel security (RHSA-2021:4356)
<a href="#">239879</a> Red Hat Update for kernel-rt (RHSA-2021:4140)
<a href="#">352334</a> Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-034
<a href="#">352335</a> Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-033
<a href="#">352336</a> Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-032
<a href="#">352337</a> Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-031
<a href="#">353100</a> Amazon Linux Security Advisory for kernel : ALAC2012-2021-024
<a href="#">353101</a> Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025

<a href="#">353102</a> Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026
<a href="#">353132</a> Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-019
<a href="#">375284</a> EulerOS Security Update for kernel (EulerOS-SA-2021-1311)
<a href="#">377055</a> Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2021:0027)
<a href="#">390233</a> Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0005)
<a href="#">610373</a> Google Android Devices October 2021 Security Patch Missing
<a href="#">610381</a> Google Android November 2021 Security Patch Missing for Huawei EMUI
<a href="#">610382</a> Google Android November 2021 Security Patch Missing for Samsung
<a href="#">610383</a> Google Android November 2021 Security Patch Missing for LGE
<a href="#">6140271</a> AWS Bottlerocket Security Update for kernel (GHSA-pjcj-m86p-4wv5)
<a href="#">670185</a> EulerOS Security Update for kernel (EulerOS-SA-2021-1684)
<a href="#">750376</a> OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)
<a href="#">750428</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0075-1)
<a href="#">750434</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0060-1)
<a href="#">900040</a> CBL-Mariner Linux Security Update for kernel 5.4.91
<a href="#">903489</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3658)
<a href="#">905763</a> Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3658-1)
<a href="#">940265</a> AlmaLinux Security Update for kernel (ALSA-2021:4356)

© [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](#)