



# CVE-2020-28941

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

## Summary

<b>CVE</b>	CVE-2020-28941
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-11-19 19:15:00 UTC
<b>Updated</b>	2023-11-07 03:21:00 UTC
<b>Description</b>	An issue was discovered in drivers/accessibility/speakup/spk_ttyio.c in the Linux kernel through 5.9.9. Local attackers on sy

## Risk And Classification

**Problem Types:** CWE-763

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## References

Reference	Source	Link	Ta
[SECURITY] Fedora 32 Update: kernel-5.9.10-100.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Th
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	Pa
oss-security - Re: Linux kernel NULL-ptr deref bug in spk_ttyio_ldisc_close	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	M
[SECURITY] Fedora 33 Update: kernel-5.9.10-200.fc33 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
speakup: Do not let the line discipline be used several times · torvalds/linux@d412275 · GitHub	MISC	<a href="https://github.com">github.com</a>	Pa
[SECURITY] Fedora 32 Update: kernel-5.9.10-100.fc32 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
kernel/git/gregkh/tty.git - TTY/Serial driver development tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>	Pa
oss-security - Linux kernel NULL-ptr deref bug in spk_ttyio_ldisc_close	MISC	<a href="https://www.openwall.com">www.openwall.com</a>	M

[SECURITY] Fedora 33 Update: kernel-5.9.10-200.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	Th
[SECURITY] [DLA 2483-1] linux-4.19 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

No vendor comments have been submitted for this CVE.

#### Legacy QID Mappings

- [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)
- [750518](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2161-1)
- [900040](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [903658](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3632)
- [905877](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3632-1)

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)