



# CVE-2020-27171

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-27171
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-03-20 22:15:00 UTC
<b>Updated</b>	2023-11-07 03:20:00 UTC
<b>Description</b>	An issue was discovered in the Linux kernel before 5.11.8. kernel/bpf/verifier.c has an off-by-one error (with a resultant inter

## Risk And Classification

**Problem Types:** CWE-193

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	All	All	All
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>	34	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## References

### Reference

- [SECURITY] [Fedora 32 Update: kernel-5.11.10-100.fc32 - package-announce - Fedora Mailing-Lists](#)
- [SECURITY] [Fedora 33 Update: kernel-5.11.8-200.fc33 - package-announce - Fedora Mailing-Lists](#)
- oss-security - Re: [CVE-2020-27171] Numeric error when restricting speculative pointer arithmetic allows unprivileged local users to leak conte
- [SECURITY] [DLA 2610-1] [linux-4.19 security update](#)
- Kernel Live Patch Security Notice LSN-0075-1 ≈ [Packet Storm](#)

[git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf.git/patch](https://git.kernel.org/pub/scm/linux/kernel/git/bpf/bpf.git/patch)

[SECURITY] Fedora 33 Update: kernel-5.11.8-200.fc33 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 34 Update: kernel-5.11.8-300.fc34 - package-announce - Fedora Mailing-Lists

[cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.11.8](https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.11.8)

oss-security - [CVE-2020-27171] Numeric error when restricting speculative pointer arithmetic allows unprivileged local users to leak content o

[SECURITY] Fedora 34 Update: kernel-5.11.8-300.fc34 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 32 Update: kernel-5.11.10-100.fc32 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[159135](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9140)

[159136](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9141)

[159179](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9222)

[159180](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9223)

[174896](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1177-1)

[174897](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1175-1)

[174916](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1210-1)

[174917](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1211-1)

[174919](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1238-1)

[178507](#) Debian Security Update for linux-4.19 (DLA 2610-1)

[198307](#) Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-5.4, Linux-azure, Linux-azure-5.4, Linux-gcp, (USN-4887-1)

[198309](#) Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-hwe, Linux-azure, Linux-azure-4.15, (USN-4890-1)

[281069](#) Fedora Security Update for kernel (FEDORA-2021-e49da8a226)

[281407](#) Fedora Security Update for kernel (FEDORA-2021-9503ffad9)

[281433](#) Fedora Security Update for kernel (FEDORA-2021-f0181b8085)

[281434](#) Fedora Security Update for kernel (FEDORA-2021-e49da8a226)

[352274](#) Amazon Linux Security Advisory for kernel: ALAS2-2021-1627

[610351](#) Google Pixel Android July 2021 Security Patch Missing

610358	Google Android July 2021 Security Patch Missing for Huawei EMUI
670416	EulerOS Security Update for kernel (EulerOS-SA-2021-1983)
670438	EulerOS Security Update for kernel (EulerOS-SA-2021-2062)
670449	EulerOS Security Update for kernel (EulerOS-SA-2021-2051)
750004	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)
750006	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)
750015	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1624-1)
750199	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)
750276	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0532-1)
750650	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)
750652	SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)
750762	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)
750766	OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)
900100	CBL-Mariner Linux Security Update for kernel 5.10.52.1
900305	CBL-Mariner Linux Security Update for kernel 5.10.57.1
900320	CBL-Mariner Linux Security Update for kernel 5.10.60.1
901643	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6526-1)
903400	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3990)
906022	Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3990-1)

© [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](#)