



# CVE-2020-8428

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

## Summary

<b>CVE</b>	CVE-2020-8428
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-29 00:15:00 UTC
<b>Updated</b>	2020-06-10 20:15:00 UTC
<b>Description</b>	fs/namei.c in the Linux kernel before 5.5 has a may_create_in_sticky use-after-free, which allows local users to cause a den

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## References

Reference	Source	Link
USN-4319-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
USN-4324-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
do_last(): fetch directory ->i_mode and ->i_uid before it's too late · torvalds/linux@d0cb501 · GitHub	MISC	<a href="https://github.com">github.com</a>
[security-announce] openSUSE-SU-2020:0336-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	<a href="https://git.kernel.org">git.kernel.org</a>
USN-4318-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
Kernel Live Patch Security Notice LSN-0065-1 ≈ Packet Storm	MISC	<a href="https://packetstormsecurity.com">packetstormsecurity.com</a>
oss-security - Re: Linux kernel: user-triggerable read-after-free crash or 1-bit infoleak oracle in open(2)	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
oss-security - Linux kernel: user-triggerable read-after-free crash or 1-bit infoleak oracle in open(2)	MISC	<a href="https://www.openwall.com">www.openwall.com</a>
Debian -- Security Information -- DSA-4667-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
[SECURITY] [DLA 2242-1] linux-4.9 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
USN-4325-1: Linux kernel vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>

USN-4320-1: Linux kernel vulnerability   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>
oss-security - Re: Linux kernel: user-triggerable read-after-free crash or 1-bit infoleak oracle in open(2)	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
Debian -- Security Information -- DSA-4698-1 linux	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>
February 2020 Linux Kernel Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</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

- [377065](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0113)
- [900078](#) CBL-Mariner Linux Security Update for kernel 5.4.91
- [902965](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3460)
- [906093](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3460-1)

© [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](https://status.cve.report)