



# CVE-2021-38198

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

## Summary

<b>CVE</b>	CVE-2021-38198
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-08-08 20:15:00 UTC
<b>Updated</b>	2022-01-04 16:38:00 UTC
<b>Description</b>	arch/x86/kvm/mmu/paging_tmpl.h in the Linux kernel before 5.12.11 incorrectly computes the access permissions of a sha

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## 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="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## References

Reference	Source	Link
KVM: X86: MMU: Use the correct inherited permissions to get shadow page · torvalds/linux@b1bd5cb · GitHub	MISC	<a href="#">github.com</a>
cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.12.11	MISC	<a href="#">cdn.kernel.org</a>
[SECURITY] [DLA 2785-1] linux-4.19 security update	MLIST	<a href="#">lists.debian.org</a>
[SECURITY] [DLA 2843-1] linux security update	MLIST	<a href="#">lists.debian.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159421](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9474)

[159422](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9475)

178844 Debian Security Update for linux-4.19 (DLA 2785-1)
178943 Debian Security Update for linux (DLA 2843-1)
180043 Debian Security Update for linux (CVE-2021-38198)
198491 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5070-1)
198541 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5114-1)
198544 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5116-1)
198546 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5116-2)
352839 Amazon Linux Security Advisory for kernel: ALAS2-2021-1704
352871 Amazon Linux Security Advisory for kernel : ALAS-2021-1539
353145 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-006
353242 Amazon Linux Security Advisory for kernel : ALAC2012-2022-036
353243 Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2022-037
353244 Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2022-038
356186 Amazon Linux Security Advisory for microvm-kernel : ALASMICROVM-KERNEL-4.14-2023-003
356218 Amazon Linux Security Advisory for microvm-kernel : ALASMICROVM-KERNEL-4.14-2023-002
671137 EulerOS Security Update for kernel (EulerOS-SA-2021-2713)
671804 EulerOS Security Update for kernel (EulerOS-SA-2022-1844)
751137 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1271-1)
751155 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3192-1)
751160 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3179-1)
751163 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3206-1)
751164 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 40 for SLE 12 SP3) (SUSE-SU-2021:3196-1)
751170 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3205-1)
751437 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3876-1)
751441 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3876-1)
751451 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3935-1)
751473 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3969-1)
751476 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3972-1)

900294 CBL-Mariner Linux Security Update for kernel 5.10.52.1
900304 CBL-Mariner Linux Security Update for kernel 5.10.57.1
900319 CBL-Mariner Linux Security Update for kernel 5.10.60.1
901372 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6582-1)
903293 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5122)
906057 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5122-1)

© [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](#)**