CVE-2021-33624

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-33624
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-23 16:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	In kernel/bpf/verifier.c in the Linux kernel before 5.12.13, a branch can be mispredicted (e.g., because of type confusion) ar

Risk And Classification

Problem Types: CWE-843

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference
oss-security - [CVE-2021-33624] Linux kernel BPF protection against speculative execution attacks can be bypassed to read arbitrary kernel r
An Analysis of Speculative Type Confusion Vulnerabilities in the Wild | USENIX
bpf: Fix leakage under speculation on mispredicted branches · torvalds/linux@9183671 · GitHub
[SECURITY] [DLA 2785-1] linux-4.19 security update
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

178844 Debian Security Update for linux-4.19 (DLA 2785-1)

179775 Debian Security Update for linux (CVE-2021-33624)

198514 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5091-1)

198515 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-1)

198521 Ubuntu Security Notification for Linux kernel (Raspberry Pi) Vulnerabilities (USN-5091-2)

198523 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-2)

198542 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5115-1)

352489 Amazon Linux Security Advisory for kernel: ALAS2-2021-1685

353145 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-006

353158 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-002

610400 Google Pixel Android March 2022 Security Patch Missing

610408 Google Android April 2022 Security Patch Missing for Huawei EMUI

670707 EulerOS Security Update for kernel (EulerOS-SA-2021-2465)

670772 EulerOS Security Update for kernel (EulerOS-SA-2021-2530)

670796 EulerOS Security Update for kernel (EulerOS-SA-2021-2554)

750828 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2305-1)

750830 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2321-1)

750832 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2324-1)

750842 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2352-1)

750864 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2421-1)

750868 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2427-1)

750869 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2422-1)

750877 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2427-1)

900096 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

901713 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6564-1)

903561 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4376)

906049 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4376-1)

© 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 registred 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