



CVE-2021-34556

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2021-34556 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-08-02 05:15:00 UTC |
| Updated | 2023-11-07 03:36:00 UTC |
| Description | In the Linux kernel through 5.13.7, an unprivileged BPF program can obtain sensitive information from kernel memory via a |

Risk And Classification

Problem Types: CWE-203

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 | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 34 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |

References

| Reference |
|---|
| [SECURITY] Fedora 34 Update: kernel-5.13.8-200.fc34 - package-announce - Fedora Mailing-Lists |
| oss-security - [CVE-2021-34556,CVE-2021-35477] Linux kernel BPF protection against Speculative Store Bypass can be bypassed to disclose |
| [SECURITY] Fedora 33 Update: kernel-5.13.8-100.fc33 - package-announce - Fedora Mailing-Lists |
| git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch |
| git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/patch |
| [SECURITY] Fedora 33 Update: kernel-5.13.8-100.fc33 - package-announce - Fedora Mailing-Lists |
| [SECURITY] [DLA 2785-1] linux-4.19 security update |
| [SECURITY] Fedora 34 Update: kernel-5.13.8-200.fc34 - package-announce - Fedora Mailing-Lists |
| 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) |
| 180199 Debian Security Update for linux (CVE-2021-34556) |
| 198515 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-1) |
| 198523 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-2) |
| 198524 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5096-1) |
| 198542 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5115-1) |
| 198563 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5137-1) |
| 198565 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5137-2) |
| 281775 Fedora Security Update for kernel (FEDORA-2021-4d4d3866ca) |
| 281780 Fedora Security Update for kernel (FEDORA-2021-54ee631709) |
| 352503 Amazon Linux Security Advisory for kernel: ALAS2-2021-1696 |
| 353156 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-004 |
| 610418 Google Pixel Android June 2022 Security Patch Missing |
| 671134 EulerOS Security Update for kernel (EulerOS-SA-2021-2688) |
| 671137 EulerOS Security Update for kernel (EulerOS-SA-2021-2713) |
| 671268 EulerOS Security Update for kernel (EulerOS-SA-2022-1196) |
| 751137 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1271-1) |
| 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) |
| 751170 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3205-1) |
| 751336 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1460-1) |
| 751349 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1477-1) |
| 751381 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:3748-1) |
| 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) |
| 900289 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 |
| 900922 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6566-1) |
| 903470 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4989) |
| 906090 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4989-1) |

© [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](#)