



CVE-2023-39194

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2023-39194 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-10-09 18:15:00 UTC |
| Updated | 2023-11-07 04:17:00 UTC |
| Description | A flaw was found in the XFRM subsystem in the Linux kernel. The specific flaw exists within the processing of state filters, v |

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|----------------------------------|---------|--------|---------|----------|
| Operating System | Fedoraproject | Fedora | 38 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | 6.5 | rc1 | All | All |
| Operating System | Linux | Linux Kernel | 6.5 | rc2 | All | All |
| Operating System | Linux | Linux Kernel | 6.5 | rc3 | All | All |
| Operating System | Linux | Linux Kernel | 6.5 | rc4 | All | All |
| Operating System | Linux | Linux Kernel | 6.5 | rc5 | All | All |
| Operating System | Linux | Linux Kernel | 6.5 | rc6 | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 9.0 | All | All | All |

References

| Reference | Source |
|--|---------|
| 2226788 – (CVE-2023-39194, ZDI-CAN-18111) CVE-2023-39194 kernel: xfrm: out-of-bounds read in __xfrm_state_filter_match() | MISC |
| ZDI-23-1492 Zero Day Initiative | MISC |
| cve-details | MISC |
| CVE Program record | CVE.ORG |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[161455](#) Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2024-12258)

[199936](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6494-1)

[199970](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6494-2)

[199976](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6534-1)

[199979](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6532-1)

[199996](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6549-1)

[199997](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6548-1)

[199999](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6548-2)

[200002](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6534-2)

[200003](#) Ubuntu Security Notification for Linux kernel (GKE) Vulnerabilities (USN-6549-2)

[200006](#) Ubuntu Security Notification for Linux kernel (Oracle) Vulnerabilities (USN-6548-3)

[200007](#) Ubuntu Security Notification for Linux kernel (Low Latency) Vulnerabilities (USN-6549-3)

[200010](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6534-3)

[200024](#) Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-6549-4)

[200035](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-6549-5)

[200037](#) Ubuntu Security Notification for Linux kernel (IoT) Vulnerabilities (USN-6548-5)

[356357](#) Amazon Linux Security Advisory for kernel : ALAS-2023-1838

[356409](#) Amazon Linux Security Advisory for kernel : ALAS2-2023-2264

[356606](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2023-053

[390296](#) Oracle VM Server for x86 Security Update for kernel (OVMSA-2024-0004)

[6000429](#) Debian Security Update for linux (DLA 3710-1)

[673534](#) EulerOS Security Update for kernel (EulerOS-SA-2024-1086)

[673595](#) EulerOS Security Update for kernel (EulerOS-SA-2023-3247)

[673644](#) EulerOS Security Update for kernel (EulerOS-SA-2023-3336)

[673660](#) EulerOS Security Update for kernel (EulerOS-SA-2023-3375)

| |
|---|
| 673692 EulerOS Security Update for kernel (EulerOS-SA-2023-3275) |
| 673923 EulerOS Security Update for kernel (EulerOS-SA-2024-1062) |
| 673995 EulerOS Security Update for kernel (EulerOS-SA-2024-1275) |
| 674042 EulerOS Security Update for kernel (EulerOS-SA-2023-3304) |
| 755059 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4035-1) |
| 755060 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4031-1) |
| 755063 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4032-1) |
| 755082 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4058-1) |
| 755083 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4057-1) |
| 755085 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4072-1) |
| 755086 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4071-1) |
| 755096 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4093-1) |
| 755229 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4072-2) |
| 755235 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2023:4377-1) |
| 755564 SUSE Security Update for the linux kernel (SUSE-SU-2023:4348-1) |
| 755565 SUSE Security Update for the linux kernel (SUSE-SU-2023:4347-1) |
| 907460 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (31268) |
| 907579 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (31268-1) |

© [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](#)