Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Critical Remote Use-After-Free Vulnerability in Linux Kernel IPv4 TCP Stack

Remote Memory Corruption	No Authentication Required	No Exploitation Observed	Fixes Rolling Out

The Cal-CSIC has become aware of a use-after-free vulnerability, CVE-2026-98432, in the IPv4 Transmission Control Protocol (TCP) connection-setup code of the Linux kernel. The kernel's TCP stack accepts every inbound connection to a Linux server, so any system exposing TCP services to untrusted networks is reachable by an attacker with no credentials.[1] The vulnerability carries a CVSS 3.1 score of 9.8 from the Linux kernel CVE team; Red Hat's own assessment is 8.1 (Important), reflecting a higher attack-complexity rating.[2,3]

When a TCP handshake completes, the kernel hands the pending request's IPv4 options to the new socket without copying them. If that socket is destroyed while another processor core still reads those options to answer a retransmitted connection request, the kernel reads freed memory.[3] A remote, unauthenticated attacker can trigger the flaw by sending crafted TCP connection requests carrying IPv4 options to any listening service but must win the race with precise timing.[1] Successful exploitation allows the attacker to crash the system or disclose and corrupt kernel memory. Open-source reporting describes an unreleased demonstration that chained a memory leak with a hijacked kernel callback to run a command as root on a server with a Multipath TCP (MPTCP) listener; Red Hat states that reliable code execution requires precise heap control.[2,4,5]

The upstream fix is included in every maintained Linux stable branch, as listed in the table below.[6] Open-source reporting as of 2 November 2026 indicates that Debian, Oracle Linux, Amazon Linux and several SUSE releases have fixed kernels while Ubuntu has none; Red Hat's bulletin of 30 October 2026 lists no fixed packages for Red Hat Enterprise Linux 8, 9 or 10 or OpenShift and states that fixes are being expedited.[1,4,6,7] Red Hat, Amazon Web Services and open-source reporting describe an interim firewall rule that drops inbound IPv4 TCP packets carrying IP options; it reduces exposure but does not fully prevent exploitation and can disrupt legitimate traffic, and disabling MPTCP alone did not block the plain-TCP path in testing.[1,4,8] Amazon Web Services states it is not aware of exploitation in the wild, the flaw was not in the CISA Known Exploited Vulnerabilities catalog as of 2 November 2026, and open-source reporting as of that date found no public proof of concept (PoC); the demonstrated exploit has not been released.[4,6,7]

The Cal-CSIC recommends that clients running self-managed Linux systems apply vendor kernel updates and reboot as soon as a fixed kernel is available for their

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

distribution, prioritizing internet-facing TCP services. Where no fixed kernel exists, clients are advised to test and deploy the interim rule that drops IPv4 TCP packets with IP options, disable MPTCP where it is not required, and monitor distribution advisories daily. Clients should also review systems for unexplained kernel crashes since 15 October 2026, when the CVE was published, and remove interim rules once patched.[1,4]

For additional details regarding CVE-2026-98432, please use this link:

Linux Kernel CVE Record:

https://nvd.nist.gov/vuln/detail/cve-2026-98432

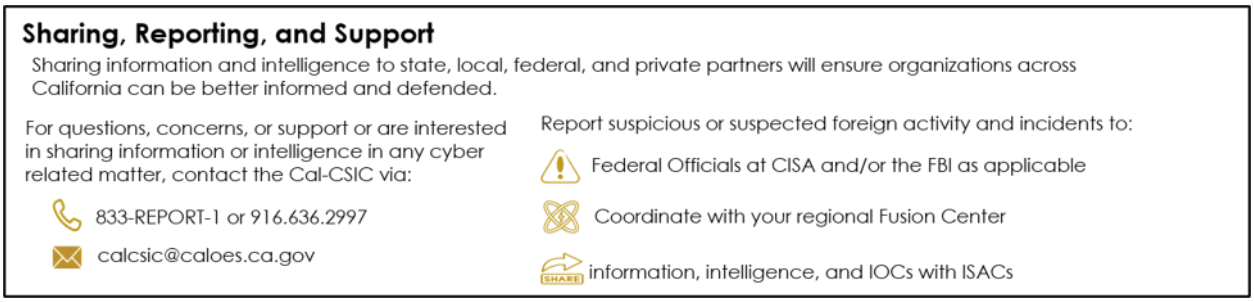
Affected Products and Versions

Product	Affected Version	Fixed Release
Linux kernel unmaintained branches (EOL)	4.4 and later branches not listed below	Vendor-backported fix or supported branch
Linux kernel 5.10.y	>=5.10 <5.10.272	5.10.272
Linux kernel 5.15.y	>=5.15 <5.15.223	5.15.223
Linux kernel 6.1.y	>=6.1 <6.1.190	6.1.190
Linux kernel 6.6.y	>=6.6 <6.6.159	6.6.159
Linux kernel 6.12.y	>=6.12 <6.12.113	6.12.113
Linux kernel 6.18.y	>=6.18 <6.18.56	6.18.56
Linux kernel 7.2.y	>=7.2 <7.2.10	7.2.10
Linux kernel 7.3 mainline	7.3-rc1 to 7.3-rc6	7.3-rc7

Versions are upstream kernel.org releases. Distribution kernels carry vendor version numbers and backported fixes, so consult the distribution advisory for the patched package. Branches at End Of Life (EOL) receive no upstream security fixes, and distributions still shipping them must backport the fix. Red Hat Enterprise Linux and Ubuntu had no fixed kernels as of 2 November 2026.[6,7]

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Sharing, Reporting, and Support



References

[1] Red Hat; "RHSB-2026-016 Use-after-free - kernel IPv4 (CVE-2026-98432)"; https://access.redhat.com/security/vulnerabilities/RHSB-2026-016; accessed 2 November 2026

[2] Red Hat; "CVE-2026-98432"; https://access.redhat.com/security/cve/cve-2026-98432; accessed 2 November 2026

[3] lilting.ch; "CVE-2026-98432 Linux TCP Use-After-Free Can Give Unauthenticated Root on MPTCP Listeners"; https://lilting.ch/en/articles/linux-ipv4-tcp-options-uaf-mptcp-rce; accessed 2 November 2026

[4] Amazon Web Services; "CVE-2026-98432 - Linux kernel IPv4 TCP use-after-free Issue"; https://aws.amazon.com/security/security-bulletins/2026-160-aws/; accessed 2 November 2026

[5] CSO Online; "Anthropic AI model finds Linux kernel bug that leads to remote root access"; https://www.csoonline.com/article/4242724/anthropic-ai-model-finds-linux-kernel-bug-that-leads-to-remote-root-access.html; accessed 2 November 2026

[6] The Hacker News; "Linux Kernel TCP Flaw With 9.8 CVSS Score Affects Ubuntu, Red Hat and Other Distributions"; https://thehackernews.com/2026/10/linux-kernel-tcp-flaw-with-98-cvss.html; accessed 2 November 2026

[7] Rescana; "Linux Kernel CVE-2026-98432: Critical TCP Use-After-Free, RHEL Fixed, Ubuntu Pending"; https://www.rescana.com/post/linux-kernel-tcp-cve-2026-98432-use-after-free-prepare-now; accessed 2 November 2026

[8] CIQ; "Mitigating CVE-2026-98432 on Rocky Linux 8, 9, 10, and LTS Variants"; https://kb.ciq.com/article/security-advisories/cve-2026-98432-mitigation; accessed 2 November 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.