CYBER ADVISORY

24 April 2025

Unauthenticated Remote Code Execution in Erlang/OTP SSH

Erlang/OTP | Remote Execution | Authentication Bypass | Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability in Erlang/OTP SSH known as CVE-2025-32433,[1] with a CVSS v3.1 score of 10.0. This vulnerability affects all users running the Erlang/OTP server and applications that provide Erlang/OTP SSH access, specifically versions prior to OTP-27.3.3, OTP-26.2.5.11, and OTP-25.3.2.20. This vulnerability allows an attacker to exploit a flaw in SSH protocol message handling and gain unauthorized access to and manipulation of sensitive data. A proof-of-concept was published by ProDefense.[2]

The CAL-CSIC recommends updating system packages.[3]

For further information on applying upgrades, please refer to Canonical Ltd.'s Security Notice or the Erlang / OTP Security Advisory.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.

Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] NIST; "CVE-2025-32433 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2025-32433; accessed 22 April 2024

[2] GitHub; "ProDefense/CVE-2025-32433"; https://github.com/ProDefense/CVE-2025-32433/blob/main/CVE-2025-32433.py; accessed 22 April 2025

[3] Github; "Unauthenticated Remote Code Execution in Erlang/OTP SSH"; https://github.com/erlang/otp/security/advisories/GHSA-37cp-fgq5-7wc2; accessed 22 April 2025