CYBER ADVISORY

TLP:CLEAR
17 MARCH 2025

Fortinet Authentication Bypass using CSF Proxy Vulnerability

Fortinet | CVE-2025-24472 | RCE | Authentication Bypass

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability, CVE-2025-24472 with a CVSS 3.x score of 9.6. CVE-2025-24472 affects two Fortinet Products: FortiOS versions 7.0.0-7.0.16 and FortiProxy version 7.2.0-7.2.12, 7.0.0-7.0.19.[1] This vulnerability allows authentication bypass using an alternate path or channel vulnerability in FortiOS and FortiProxy. A remote user can craft ConfigServer Firewall (CSF) proxy requests to gain super-admin privileges. A Proof-of-Concept has been disclosed, and this vulnerability is confirmed to be exploited in the wild.[2] [3]

The Cal-CSIC recommends immediately updating to the latest version.

For further information on applying these updates please refer to Fortinet PSIRT 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. To help us identify ways to better assist you, please submit feedback here.
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.

[1] FortiGuard Labs; "Authentication bypass in Node.js websocket module and CSF requests" https://www.fortiguard.com/psirt/FG-IR-24-535; accessed 17 March 2025

[2] Forescout; " New Ransomware Operator Exploits Fortinet Vulnerability Duo"; https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/?utm_source=chatgpt.com; accessed 17 March 2025

[3] Avertium; "Flash Notice: CVE-2025-24472 Actively Exploited - Patch and Manage" https://www.avertium.com/flash-notices/cve-2025-24472-actively-exploited-patch-and-manage; accessed 17 March 2025