



CYBER ADVISORY



Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

TLP: CLEAR

May 29, 2025

Missing Authentication for Critical Function Vulnerability in Fortinet Products

CVE-2025-22252

FortiOS

FortiSwitchManager

FortiProxy

The California Cybersecurity Integration Center (Cal-CSIC) has identified an existing Missing Authentication for Critical Function Vulnerability (CVE-2025-22252) that allows a remote threat actor to bypass authentication. Currently there is no known exploitation in the wild, nor is the exploit code available for the public. CVE 2025-22252 affects Fortinet FortiProxy versions 7.6.0 through 7.6.1, FortiSwitchManager version 7.2.5, and FortiOS versions 7.4.4 through 7.4.6, and 7.6.0. ¹

Successful exploitation of CVE-2025-22252 may allow a threat actor with knowledge of an existing admin account to access the device as a valid admin via authentication bypass. This vulnerability is limited to configurations where ASCII authentication is used. PAP, MSCHAP, and CHAP configurations are not impacted. ²

Title	CVE (CVSS 3.1)	Description	Affected products
Missing Authentication for Critical Function Vulnerability	CVE-2025-22252(9.8)	A missing authentication for critical function that allows an attacker with knowledge of an existing admin account to access the device as a valid admin via an authentication bypass. ³	Fortinet FortiProxy versions 7.6.0 to 7.6.1 Fortinet SwitchManager version 7.2.5 FortiOS versions 7.4.4 to 7.4.6 and 7.6.0

CAL-CSIC-202505-007

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.

TLP: CLEAR

The Cal-CSIC recommends immediately applying the appropriate updates and/or workarounds provided by Fortinet to vulnerable products.

For more information on applying the security updates and/or workarounds, please refer to [PSIRT | FortiGuard Labs](#).

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 NIST National Vulnerability Database; "CVE-2025-22252 Detail"; <https://nvd.nist.gov/vuln/detail/CVE-2025-22252>; accessed 29 May 2025

² FortiGuard Labs; "TACACS+ Authentication Bypass"; <https://fortiguard.fortinet.com/psirt/FG-IR-24-472>; accessed 29 May 2025

³ MITRE CVE; "CVE-2025-22252"; <https://cve.mitre.org/cgi-bin/cvename.cgi?name=2025-22252>; accessed 29 May 2025