



CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

TLP:CLEAR

08 February 2024

FortiOS Vulnerability

CVE-2024-21762

Out-of-Bounds

RCE

Critical Vulnerability

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability, likely under active exploitation known as CVE-2024-21762. The vulnerability affects Fortinet's FortiOS.¹ The out-of-bounds write vulnerability may allow a remote unauthenticated attacker to execute arbitrary code or command via specially crafted HTTP requests.²

Version	Affected	Solution
FortiOS 7.6	Not affected	Not Applicable
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiOS 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above
FortiOS 6.0	6.0 all versions	Migrate to a fixed release

Table 1: Affected Versions and Solutions for FortiOS

The Cal-CSIC recommends to immediately disable SSL VPN (disable webmode is NOT a valid workaround) and apply appropriated upgrades.

For further information on applying upgrades, please refer to [Fortinet Upgrade Path Tool](#).

CAL-CSIC-202402-004

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR

PUBLIC SERVICE ANNOUNCEMENT

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

TLP:CLEAR

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 calcsic@caloes.ca.gov .
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 Bleeping Computer; "New Fortinet RCE flaw in SSL VPN likely exploited in attacks;" <https://www.bleepingcomputer.com/news/security/new-fortinet-rce-flaw-in-ssl-vpn-likely-exploited-in-attacks/>; accessed 08 February 2024

² FortiGuard Labs; "FortiOS - Out-of-bound Write in sslvpnd;" <https://www.fortiguard.com/psirt/FG-IR-24-015>; accessed 08 February 2024

CAL-CSIC-202402-004

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

TLP:CLEAR