CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CYBER ADVISORY

TLP:CLEAR
16 May 2025

Fortinet Stack-Based Buffer Overflow Vulnerability

Fortinet | Stack Overflow | Remote Code Execution | Active Exploitation

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability known as CVE-2025-32756 with a CVSS 3.1 score of 9.8.[1] This vulnerability allows an attacker to create a stack overflow and subsequently execute remote code.[1] This vulnerability applies to multiple Fortinet products and versions including FortiVoice, FortiRecorder, FortiMail, FortiNDR, and FortiCamera.[2] See below for breakdown of affected product versions. Fortinet has observed the vulnerability being exploited in the wild specifically on FortiVoice but the other products are susceptible.[23]

Title	CVE (CVSS Score)	Description	Affected Versions
Fortinet Stack-Based Buffer Overflow Vulnerability	CVE-2024-32756 (**9.8**)	Stack-based overflow vulnerability; allows a remote unauthenticated attacker to execute binary code or commands via sending HTTP requests with specially crafted hash cookie.	FortiVoice versions: 7.2.0, 7.0.0 through 7.0.6, 6.4.0 through 6.4.10, FortiRecorder versions: 7.2.0 through 7.2.3, 7.0.0 through 7.0.5, 6.4.0 through 6.4.5 FortiMail versions: 7.6.0 through 7.6.2, 7.4.0 through 7.4.4, 7.2.0 through 7.2.7, 7.0.0 through 7.0.8 FortiNDR versions: 7.6.0, 7.4.0 through 7.4.7, 7.2.0 through 7.2.4, 7.0.0 through 7.0.6 FortiCamera versions: 2.1.0 through 2.1.3, 2.0 all versions, 1.1 all versions

The Cal-SCIC recommends upgrading and/or migrating software to the latest versions.[2] If applying an upgrade is not available, a temporary option is to disable HTTP/HTTPS administrative interface.[2]

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.

For further information on applying upgrades please refer to the Fortinet 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-2025-32756 Detail; https://nvd.nist.gov/vuln/detail/CVE-2025-32756; accessed 15 May 2025

[2] Fortinet; Stack-based buffer overflow vulnerability in API; https://fortiguard.fortinet.com/psirt/FG-IR-25-254; accessed 15 May 2025

[3] CISA; Known Exploited Vulnerabilities Catalog; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=2025-32756&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=; accessed 15 May 2025