



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Friday October 02, 2026

CAL-CSIC-202610-A-003

Critical Vulnerability on Fortinet FortiMail Path Traversal

Remote Code Execution

No Authentication

Actively Exploited

FortiMail

The California Cybersecurity Integration Center (Cal-CSIC) have identified a critical zero-day vulnerability, CVE-2026-104286, affecting Fortinet FortiMail appliances. CVE-2026-104286 involves path traversal (CWE-22) and improper neutralization of NULL bytes (CWE-158) in the web management interface, which allows an unauthenticated remote attacker to write arbitrary files on the underlying operating system via crafted HTTP or HTTPS requests, potentially achieving arbitrary code execution.¹ Exploitation requires no authentication, administrative credentials, or user interaction. The vulnerability carries a CVSS v3.1 base score of 9.8 (Critical)² and has been added to the CISA Known Exploited Vulnerabilities (KEV)³ catalog due to confirmed active exploitation in the wild.

The Cal-CSIC recommends following [Fortinet Advisory](#):

1. Restrict Management Access Immediately: Disable access to the FortiMail administrative web interface (HTTP/HTTPS) from the public internet or restrict access exclusively to trusted private administrative subnets or management VPNs.
2. Apply Vendor Updates / Plan Branch Upgrades: Upgrade affected appliances to the fixed software versions once available (8.0.2, 7.6.7, or 7.4.9). Deployments on the 7.2.x train should plan an upgrade path to the supported 7.4 branch or above.
3. Inspect for Indicators of Compromise (IoCs): Review web server access logs for anomalous HTTP/HTTPS POST requests containing path traversal sequences (such as ../ or %00 NULL-byte encoding) and inspect appliance storage for unauthorized web shells or unfamiliar script files.

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

Affected Components, Versions, and Solution

Affected Version	Affected Range	Solution
FortiMail 8.0	8.0.0 through 8.0.1	Upgrade to upcoming 8.0.2 or above
FortiMail 7.6	7.6.0 through 7.6.6	Upgrade to upcoming 7.6.7 or above
FortiMail 7.4	7.4.0 through 7.4.8	Upgrade to upcoming 7.4.9 or above
FortiMail 7.2	7.2.0 through 7.2.9	Upgrade to branch 7.4 or above

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

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

References:

¹ CVE; "CVE-2026-104286"; <https://www.cve.org/CVERecord?id=CVE-2026-104286>; accessed 02 October 2026

² FortiGuard Labs; "Improper limitation of a pathname to a restricted directory"; <https://fortiguard.fortinet.com/psirt/FG-IR-26-175>; accessed 02 October 2026

³ CISA; "Known Exploited Vulnerabilities Catalog"; https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-104286; accessed 02 October 2026

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