



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Monday, March 30, 2026

CAL-CSIC-202603-A-010

Fortinet FortiClient EMS RCE Vulnerability Currently Under Active Exploitation

Crafted HTTP Request

SQL Injection

Remote Code Execution

Patch Available

This is the first update to the CAL-CSIC-202602-A-005 advisory, published on 09 February 2026. It is based on CVE-2026-21643 which carries a CVSS 3.1 score of 9.8, allowing an unauthenticated remote attacker to execute arbitrary code via specially crafted HTTP requests¹. This vulnerability is currently being actively exploited in the wild as discovered by Defused cyber researchers². The vendor has issued a security advisory with patching and mitigation instructions.

The Cal-CSIC strongly recommends all organizations follow the vendor's guidance in mitigation, to include immediate patching. For further information on Fortinet's security advisory and analysis please use this link:

Security Advisory

<https://fortiguard.fortinet.com/psirt/FG-IR-25-1142>

Affected Product:

Product Name	Affected Version	Solution
FortinetClient FortiClient	7.4.4	Upgrade to 7.4.5 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 NVD; “CVE-2026-21643 Detail”; <https://nvd.nist.gov/vuln/detail/CVE-2026-21643>; accessed 30 March 2026

² Security Affairs; “Attackers are exploiting a critical Fortinet FortiClient EMS flaw (CVE-2026-21643) that allows remote code execution via SQL injection”; <https://securityaffairs.com/190158/security/critical-fortinet-forticlient-ems-flaw-exploited-for-remote-code-execution.html>; accessed 30 March 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