



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

Monday, February 9, 2026

CSIC-ADVISORY-202602-A-010

Fortinet FortiClientEMS SQL Injection Vulnerability

Crafted HTTP Request

Unauthenticated Attacker

Unauthorized Code

Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability impacting Fortinet FortiClientEMS. CVE-2026-21643 carries a CVSS 3.1 score of 9.8.¹ Successful exploitation allows an unauthenticated attacker to execute unauthorized code or commands via specially crafted HTTP requests.² The attacker would potentially be able to gain high-level access to sensitive data, modify system configurations, or deploy malware.

CVE-2026-21643 has not been confirmed to be exploited in the wild and not as a zero-day. The vendor has issued a security advisory with patching and mitigation instructions.

The Cal-CSIC recommends immediately following the vendor's guidance in mitigation, to include immediate patching.³ For further information on Fortinet's security advisory and analysis please use these links:

Security Advisory

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

Affected Product:

Product Name	Affected Version	Solution
Fortinet FortiClient	7.4.4	Upgrade to 7.4.5 or above

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 9 February 2026

² Tenable; “CVE-2026-21643” <https://www.tenable.com/cve/CVE-2026-21643>; accessed 9 February 2026

³ FortiGuard Labs; “SQLi in administrative interface”; <https://fortiguard.fortinet.com/psirt/FG-IR-25-1142>; accessed 9 February 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