



CYBER ADVISORY

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



CYBER ADVISORY

TLP:CLEAR

14 July 2025

Fortinet FortiWeb Fabric Connector SQL Injection

Fortinet

RCE

PoC

SQL Injection

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability affecting the Fortinet FortiWeb Fabric Connector. The Fabric Connector facilitates communication between FortiWeb and other components within the Fortinet Security Fabric, such as FortiGate and FortiAnalyzer, enabling the exchange of threat intelligence and automation of security policies.¹ This vulnerability, identified as CVE-2025-25257 with a CVSS v3.0 score of 9.8, stems from improper neutralization of special elements in SQL commands. If exploited, it could allow a remote attacker to execute arbitrary code via crafted HTTP or HTTPS requests.² A proof-of-concept for this vulnerability has been publicly disclosed by watchTowr Labs.³

Affected Versions:

- 7.6.0 through 7.6.3
- 7.4.0 through 7.4.7
- 7.2.0 through 7.2.10
- 7.0.0 through 7.0.10

The Cal-CSIC recommends immediately applying the latest versions of FortiWeb due to the severity of this vulnerability.

For more information on applying the latest security updates, please refer to [Fortinet's administration guide](#)

CAL-CSIC-202507-002

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

CYBER ADVISORY

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.
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.

¹ Fortinet; “Fabric Connectors” <https://www.fortinet.com/solutions/enterprise-midsize-business/fabric-connectors>; accessed 14 July 2025

² FortiGuard Labs; “Unauthenticated SQL injection in GUI” <https://fortiguard.fortinet.com/psirt/FG-IR-25-151>; accessed 14 July 2025

³ watchTowr Labs; “Pre-Auth SQL Injection to RCE - Fortinet FortiWeb Fabric Connector (CVE-2025-25257)” <https://labs.watchtowr.com/pre-auth-sql-injection-to-rce-fortinet-fortiweb-fabric-connector-cve-2025-25257/>; accessed 14 July 2025

CAL-CSIC-202507-002

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