CALIFORNIA CYBERSECURITY INTEGRATION CENTER

CYBER ADVISORY

Friday, August 15, 2025 CSIC-ADVISORY-202508-001

FortiSIEM Remote Unauthenticated Command Injection Vulnerability

FortiSIEM | Improper Neutralization | OS Command Injection | Command Line Interface

The California Cybersecurity Integration Center (Cal-CSIC) has identified a critical vulnerability affecting Fortinet Security Information and Event Management (FortiSIEM) product. CVE-2025-25256, assigned a CVSS v3.0 score of 9.8, arises from improper neutralization of special elements used in operating system commands also known as OS Command Injection (CWE-78)[i]. Successful exploitation could allow a remote, unauthenticated attacker to execute unauthorized code or commands through crafted command line interface requests. [ii] Fortinet has observed the vulnerability being exploited in the wild. [iii]

Affected Versions:

FortiSIEM 7.3	7.3.0 through 7.3.1
FortiSIEM 7.2	7.2.0 through 7.2.5
FortiSIEM 7.1	7.1.0 through 7.1.7
FortiSIEM 7.0	7.0.0 through 7.0.3
FortiSIEM 6.7	6.70 through 6.7.9
FortiSIEM 6.6	All versions

The Cal-CSIC recommends immediately applying the mitigations provided by Fortinet's security bulletin due to the severity of the vulnerability and active exploitation documented in the wild.

Fortinet Security Bulletin CVE-2025-25256

References

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.

[i] National Vulnerability Database; “CVE-2025-25256 Detail” https://nvd.nist.gov/vuln/detail/CVE-2025-25256; accessed 14 August 2025

[ii] Hacker News; “Fortinet Warns About FortiSIEM Vulnerability (CVE-2025-25256) With In-the-Wild Exploit Code” https://thehackernews.com/2025/08/fortinet-warns-about-fortisiem.html; accessed 14 August 2025

[iii] Fortiguard; “Remote Unauthenticated Command Injection” https://fortiguard.fortinet.com/psirt/FG-IR-25-152; accessed 14 August 2025