مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical SQL Injection Vulnerability in FortiWeb

Tracking #:432317468

Date:09-07-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Fortinet has disclosed a critical SQL injection vulnerability in multiple versions of its FortiWeb product.

TECHNICAL DETAILS:

Fortinet has disclosed a critical SQL injection vulnerability (CVE-2025-25257) in multiple versions of its FortiWeb product. This vulnerability allows unauthenticated remote attackers to execute arbitrary SQL commands through specially crafted HTTP or HTTPS requests targeting the GUI administrative interface.

The issue stems from improper sanitization of SQL inputs (CWE-89) and can lead to full system compromise, data theft, or unauthorized access to backend systems.

Given the critical nature (CVSS 9.6) and the fact that exploitation requires no authentication, organizations using affected FortiWeb versions are urged to take immediate action.

Vulnerability Details:

- CVE ID: **CVE-2025-25257**
- CVSSv3 Score: 9.6 (Critical)
- Component: FortiWeb GUI (Administrative Web Interface)
- Impact:
  - Unauthorized execution of SQL queries
  - Potential full compromise of the FortiWeb appliance
  - Unauthorized access to sensitive configuration and user data
- Attack Vector: Remote via crafted HTTP/HTTPS requests
- Authentication Required: No
- Root Cause: Improper neutralization of special elements used in SQL commands (CWE-89)

Affected Products & Fixed version:

Version	Affected	Solution
FortiWeb 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiWeb 7.4	7.4.0 through 7.4.7	Upgrade to 7.4.8 or above
FortiWeb 7.2	7.2.0 through 7.2.10	Upgrade to 7.2.11 or above
FortiWeb 7.0	7.0.0 through 7.0.10	Upgrade to 7.0.11 or above

- Workaround: Disable HTTP/HTTPS administrative interface

RECOMMENDATIONS:

- Apply Official Patches Upgrade FortiWeb to a non-vulnerable version as specified above.
- Restrict access to the management interface by disabling remote GUI access over HTTP/HTTPS if immediate upgrade is not feasible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.fortiguard.com/psirt/FG-IR-25-151