مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in FortiClientEMS

Tracking #:432318371

Date:09-02-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in FortiClientEMS that may allow unauthorized code or command execution on affected systems.

TECHNICAL DETAILS:

A critical SQL Injection vulnerability has been identified in the administrative interface of FortiClientEMS. The flaw is caused by improper neutralization of special elements in SQL commands and may allow an unauthenticated attacker to execute unauthorized code or commands by sending specially crafted HTTP requests.

Vulnerability Details

- **CVE-2026-21643**
- **CVSS v3 Score:** 9.1 Critical
- The vulnerability exists due to insufficient input validation in the FortiClientEMS administrative interface. An unauthenticated remote attacker could exploit this flaw by injecting malicious SQL statements via crafted HTTP requests, potentially leading to unauthorized command execution on the affected system.

Affected Versions

- FortiClientEMS 7.4.4

Fixed Versions

- FortiClientEMS 7.4.5 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Fortinet.

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