مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

OS Command Injection Vulnerability in Fortinet FortiDDoS-F

Tracking #:432317693

Date:11-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in Fortinet FortiDDoS-F appliances that could be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Fortinet has disclosed a medium-severity OS command injection vulnerability affecting FortiDDoS-F appliances. Tracked as CVE-2024-45325 with a CVSS v3.1 score of 6.5, this flaw can allow attackers with privileged access to execute unauthorized commands via specially crafted CLI requests. Successful exploitation may compromise the confidentiality, integrity, and availability of affected systems, undermining critical DDoS protection infrastructure.

Vulnerability Details

- **CVE-2024-45325**
- Severity: Medium
- CVSS v3.1 Score: 6.5
- Vulnerability Type: OS Command Injection (CWE-78)
- Affected Component: FortiDDoS-F Command-Line Interface (CLI)
- Attack Vector: Local (privileged access required)
- Impact: Allows execution of unauthorized commands, risking system compromise and disabling DDoS defenses.

Affected Versions:

- FortiDDoS-F 7.0.0 – 7.0.2
- FortiDDoS-F 6.1 – 6.6 (all)

Fixed Versions:

- FortiDDoS-F 7.0 update to version 7.0.3 or later.
- FortiDDoS-F 6.1–6.6 deployments migrate to supported fixed releases

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-24-344