مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Fortinet Products

Tracking #:432316860

Date:12-02-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet has identified and disclosed two high-severity vulnerabilities affecting FortiOS and FortiPortal.

TECHNICAL DETAILS:

Fortinet has identified and disclosed two high-severity vulnerabilities affecting FortiOS and FortiPortal. These vulnerabilities could allow attackers to escalate privileges to super-admin level or retrieve sensitive source code, respectively.

Key Vulnerabilities

1. **CVE-2024-40591: Improper Privilege Management in FortiOS**
   - **CVSSv3 Score:** 8.0 (High)
   - **Impact:** Privilege Escalation
   - **Description:** An authenticated admin with Security Fabric permissions can exploit this vulnerability by connecting a targeted FortiGate device to a malicious upstream FortiGate under their control. This could allow the attacker to escalate their privileges to super-admin, gaining full control over the system.
   - **Affected Versions:**
     - FortiOS 7.6.0
     - FortiOS 7.4.0 through 7.4.4
     - FortiOS 7.2.0 through 7.2.9
     - FortiOS 7.0.0 through 7.0.15
     - FortiOS 6.4 (all versions)
   - **Fixed Versions:**
     - FortiOS 7.6.1 or above
     - FortiOS 7.4.5 or above
     - FortiOS 7.2.10 or above
     - FortiOS 7.0.16 or above
     - Migrate from FortiOS 6.4 to a fixed release.

2. **CVE-2025-24470: Off-by-Slash Vulnerability in FortiPortal**
   - **CVSSv3 Score:** 8.1 (High)
   - **Impact:** Information Disclosure
   - **Description:** A remote, unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests to retrieve sensitive source code from the FortiPortal system. This could lead to further exploitation or compromise of the system.
   - **Affected Versions:**
     - FortiPortal 7.4.0 through 7.4.2
     - FortiPortal 7.2.0 through 7.2.6
     - FortiPortal 7.0.0 through 7.0.11
   - **Fixed Versions:**
     - FortiPortal 7.4.3 or above
     - FortiPortal 7.2.7 or above
     - FortiPortal 7.0.12 or above.

RECOMMENDATIONS:

- Organizations are strongly encouraged to apply the recommended updates and monitor for any signs of exploitation.

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-24-302
- https://fortiguard.fortinet.com/psirt/FG-IR-25-015