مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Exploited Vulnerability in FortiOS and FortiProxy

Tracking #:432316997

Date:21-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Fortinet FortiOS and FortiProxy has been exploited wild.

TECHNICAL DETAILS:

Fortinet has identified a severe vulnerability in FortiOS and FortiProxy that allows unauthenticated remote attackers to bypass authentication mechanisms and gain "super-admin" privileges. This critical flaw has been actively exploited in the wild. Fortinet has observed threat actors performing malicious post-exploitation activities, including the creation of random administrative and local user accounts, modification of system configurations (e.g., firewall policies), and the use of SSL VPN for unauthorized access to internal network.

- CVE Identifier: **CVE-2025-24472 & CVE-2024-55591**
- Severity: CVSSv3 Score 9.6 Critical
- Vulnerability Type: Authentication Bypass (CWE-288)
- Impact: Remote unauthenticated attackers can gain super-admin access to FortiOS and FortiProxy devices.

- **Affected Versions**
  - FortiOS 7.0.0 through 7.0.16
  - FortiProxy 7.0.0 through 7.0.19
  - FortiProxy 7.2.0 through 7.2.12

- **Mitigation**
  - FortiOS 7.0: Upgrade to 7.0.17 or above
  - FortiProxy 7.0: Upgrade to 7.0.20 or above
  - FortiProxy 7.2: Upgrade to 7.2.13 or above

If immediate upgrade is not possible:

  - Disable HTTP/HTTPS administrative interface
  - Limit IP addresses that can access the administrative interface using local-in policies

- **Threat Actor Activities**

Attackers exploiting this vulnerability have been observed:

  - Creating random admin or local user accounts
  - Adding users to existing or new SSL VPN user groups
  - Modifying firewall policies and other settings
  - Logging into SSL VPN using created accounts to access internal networks

- **Indicators of Compromise**
  - Suspicious login activities with random source and destination IPs
  - Admin creation logs with randomly generated usernames
  - Commonly used attacker IP addresses: 1.1.1.1, 127.0.0.1, 2.2.2.2, 8.8.8.8, 8.8.4.4
  - Known attacker IP addresses:
  - 45.55.158.47 (most used)
  - 87.249.138.47
  - 155.133.4.175

- 37.19.196.65
- 149.22.94.37

RECOMMENDATIONS:

- Upgrade affected systems immediately,if immediate upgrade is not possible, implement the mentioned mitigations.
- Monitor systems for indicators of compromise and Conduct a thorough security assessment of potentially affected systems.

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-24-535