مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Fortinet

Tracking #:432317597

Date:13-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Fortinet has released security updates addressing multiple vulnerabilities affecting FortiSIEM, FortiOS, FortiProxy, FortiPAM, and FortiWeb products. These vulnerabilities may allow unauthenticated attackers to execute commands, bypass authentication, or gain unauthorized access to devices and sensitive data.

TECHNICAL DETAILS:

Vulnerability Details:

1. **CVE-2025-25256** - Remote unauthenticated command injection
   - **Severity:** Critical
   - **CVSS Score:** 9.8
   - Description: Improper neutralization of special elements used in OS commands ("OS Command Injection") may allow an unauthenticated attacker to execute arbitrary commands on affected systems via crafted CLI requests. Exploit code has been observed in the wild.
   - Impact: Full system compromise, data exfiltration, and unauthorized command execution on vulnerable FortiSIEM devices.

2. **CVE-2024-26009** - Weak authentication - FGFM protocol
   - **Severity:** High
   - **CVSS Score:** 7.9
   - Description: An authentication bypass using an alternate path or channel vulnerability may allow an unauthenticated attacker to seize control of a managed device via crafted FGFM requests.
   - Impact: Unauthorized access to managed devices, potential takeover of device functionality, and compromise of network security.

3. **CVE-2025-52970** - Authentication bypass via invalid parameter
   - **Severity:** High
   - **CVSS Score:** 7.7
   - Description: Improper handling of parameters may allow an unauthenticated attacker with knowledge of non-public information to log in as any existing user on the device via specially crafted requests.
   - Impact: Unauthorized user access, potential data exposure, and elevated privilege attacks on FortiWeb devices.

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
FortiSIEM 7.3	7.3.0 through 7.3.1	Upgrade to 7.3.2 or above
FortiSIEM 7.2	7.2.0 through 7.2.5	Upgrade to 7.2.6 or above

FortiSIEM 7.1	7.1.0 through 7.1.7	Upgrade to 7.1.8 or above
FortiSIEM 7.0	7.0.0 through 7.0.3	Upgrade to 7.0.4 or above
FortiSIEM 6.7	6.7.0 through 6.7.9	Upgrade to 6.7.10 or above
FortiOS 6.4	6.4.0 through 6.4.15	Upgrade to 6.4.16 or above
FortiOS 6.2	6.2.0 through 6.2.16	Upgrade to 6.2.17 or above
FortiOS 6.0	6.0 all versions	Migrate to a fixed release
FortiPAM 1.2	1.2 all versions	Migrate to a fixed release
FortiPAM 1.1	1.1 all versions	Migrate to a fixed release
FortiPAM 1.0	1.0 all versions	Migrate to a fixed release
FortiProxy 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiProxy 7.2	7.2.0 through 7.2.8	Upgrade to 7.2.9 or above
FortiProxy 7.0	7.0.0 through 7.0.15	Upgrade to 7.0.16 or above
FortiSwitchManager 7.2	7.2.0 through 7.2.3	Upgrade to 7.2.4 or above
FortiSwitchManager 7.0	7.0.0 through 7.0.3	Upgrade to 7.0.4 or above

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-25-152
- https://fortiguard.fortinet.com/psirt/FG-IR-24-042
- https://fortiguard.fortinet.com/psirt/FG-IR-25-448