مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Fortinet Products

Tracking #:432319299

Date:16-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet has released multiple security advisories addressing seven vulnerabilities affecting several products, including FortiOS, FortiProxy, FortiPAM, FortiSandbox, and FortiSASE.

TECHNICAL DETAILS:

Fortinet has released multiple security advisories addressing seven vulnerabilities affecting several products, including FortiOS, FortiProxy, FortiPAM, FortiSandbox, and FortiSASE. The vulnerabilities range from Low to High severity and include unauthenticated VNC access, stack-based buffer overflow, reflected cross-site scripting (XSS), path traversal, buffer over-read, and HTTP header injection vulnerabilities.
The most severe issue, CVE-2026-59835, affects FortiSandbox and could allow unauthenticated attackers to access the Virtual Network Computing (VNC) service exposed on all network interfaces, potentially enabling unauthorized access to sandbox sessions.

Vulnerability Details:

1. CVE-2026-59835 – Unauthenticated VNC Access Exposed on All Interfaces (High)

Affected Products:

- FortiSandbox: 5.2, 5.0, 4.4

2. CVE-2026-59837 – Stack Buffer Overflow in Log Report (Medium)

Affected Products:

- FortiOS: 8.0, 7.6, 7.4, 7.2
- FortiPAM: 1.9, 1.8, 1.7, 1.6, 1.5
- FortiProxy: 7.6, 7.4, 7.2

3. CVE-2026-23573 – SSL-VPN Reflected Cross-Site Scripting (Medium)

Affected Products:

- FortiOS: 8.0, 7.6, 7.4, 7.2
- FortiPAM: 1.9, 1.8, 1.7, 1.6, 1.5
- FortiProxy: 7.6, 7.4, 7.2

4. CVE-2026-59839 – Path Traversal in CLI Command Allows Deletion of Root File System (Medium)

Affected Products:

- FortiOS: 8.0, 7.6, 7.4, 7.2, 7.0
- FortiPAM: 1.8, 1.7, 1.6, 1.5, 1.4
- FortiProxy: 7.6, 7.4, 7.2, 7.0

5. CVE-2025-62675 – Header Injection in Web Filter Warning Page (Low)

Affected Products:

- FortiOS: 8.0, 7.6, 7.4, 7.2
- FortiProxy: 7.6, 7.4, 7.2

6. CVE-2025-62826 – Header Injection in Captive Portal Authentication Form (Low)

Affected Products:

- FortiOS: 7.6, 7.4, 7.2
- FortiProxy: 7.6, 7.4, 7.2

7. CVE-2025-43892 – Buffer Over-Read in authd and wad Daemons (Medium)

Affected Products:

- FortiOS: 7.6, 7.4, 7.2
- FortiProxy: 7.6, 7.4, 7.2
- FortiSASE

RECOMMENDATIONS:

Immediate Actions:

- Immediately apply the latest Fortinet security updates for affected products.
- Prioritize remediation of FortiSandbox (CVE-2026-59835) due to its unauthenticated nature.

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