مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Fortinet Products

Tracking #:432318790

Date:15-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple critical vulnerabilities have been identified across a wide range of Fortinet products, including FortiOS, FortiManager, FortiAnalyzer, and FortiSandbox.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been identified across a wide range of Fortinet products, including FortiOS, FortiManager, FortiAnalyzer, and FortiSandbox. The most critical issues enable remote code execution (RCE) and unauthorized system access. Attackers can leverage these flaws to gain initial access, execute arbitrary commands, exfiltrate sensitive data, and potentially achieve full system compromise.

Critical & High-Severity Vulnerabilities

- **Heap-Based Buffer Overflow (CWE-122)**
  - CVE-2026-22828 (FortiAnalyzer Cloud)
  - Unauthenticated RCE via crafted requests to oftpd daemon
- **OS Command Injection (CWE-78)**
  - CVE-2026-39808 (FortiSandbox)
  - Remote unauthenticated execution via malicious HTTP requests
  - Affected Versions FortiSandbox -4.4 4.4.0 through 4.4.8
  - Fixed: 4.4.9 or above
- **SQL Injection (CWE-89)**
  - CVE-2026-39809 (FortiClientEMS)
  - Authenticated attackers can execute arbitrary SQL queries
  - CVE-2026-39815 (FortiDDoS-F) – similar impact
- **Authentication Bypass / Path Traversal (CWE-24 / CWE-22)**
  - CVE-2026-39813 (FortiSandbox API)
  - Enables bypass of authentication controls
  - Affected versions FortiSandbox 5.0 5.0.0 through 5.0.5,FortiSandbox 4.4 4.4.0 through 4.4.8
  - Fixed-5.0.6 or above, 4.4.9 or above

Additional Notable Vulnerabilities

- **Authentication Bypass (2FA Replay)**
  - CVE-2026-23708 (FortiSOAR)
- **Credential Exposure / Weak Storage**
  - CVE-2026-22574, CVE-2026-22576 (FortiSOAR)
  - CVE-2026-39810 (Hardcoded crypto key in FortiClientEMS)
- **Cleartext Sensitive Data Transmission**
  - CVE-2026-21742, CVE-2026-22155
- **Server-Side Request Forgery (SSRF)**
  - CVE-2025-59809 (FortiSOAR)
- **Cross-Site Scripting (XSS)**
  - Multiple CVEs across FortiSandbox and FortiSOAR
- **Denial of Service (DoS)**
  - CVE-2026-39811 (FortiWeb – Integer Overflow)

- **Path Traversal Leading to Arbitrary File Operations**
  - CVE-2025-61624 (FortiOS, FortiPAM, FortiProxy, FortiSwitchManager)
  - Arbitrary file write/delete via CLI

RECOMMENDATIONS:

- Immediate Actions:
  - Apply latest Fortinet patches/firmware updates immediately.
  - Prioritize systems exposed to the internet (FortiOS, FortiManager, FortiAnalyzer)

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