مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Fortinet Security Updates

Tracking #:432318947

Date:13-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet has disclosed multiple high-severity and critical vulnerabilities affecting several enterprise security products including Fortinet products such as FortiOS, FortiAuthenticator, and FortiSandbox.

TECHNICAL DETAILS:

Fortinet has disclosed multiple high-severity and critical vulnerabilities affecting several enterprise security products including Fortinet products such as FortiOS, FortiAuthenticator, and FortiSandbox. The vulnerabilities could allow authenticated or unauthenticated attackers to execute arbitrary code or commands on affected systems. The issues impact wireless controller services, API endpoints, and web UI authorization mechanisms.

1. FortiOS:

Vulnerability Details

- **CVE ID:** CVE-2025-53844
- **IR Number:** FG-IR-26-123
- **Severity:** High
- **CVSS v3 Score:** 8.3
- An Out-Of-Bounds Write vulnerability [CWE-787] in FortiOS capwap daemon may allow an attacker controlling an authenticated FortiAP FortiExtender or FortiSwitch to gain execution privileges on the FortiGate device

Version	Affected	Solution
FortiOS 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiOS 7.4	7.4.0 through 7.4.8	Upgrade to 7.4.9 or above
FortiOS 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above

2. FortiAuthenticator:

Vulnerability Details

- **CVE ID:** CVE-2026-44277
- **IR Number:** FG-IR-26-128
- **Severity:** Critical
- **CVSS v3 Score:** 9.1
- **CWE:** CWE-284 – Improper Access Control
- An Improper Access Control vulnerability [CWE-284] in FortiAuthenticator may allow an unauthenticated attacker to execute unauthorized code or commands via crafted requests.

Version	Affected	Solution
FortiAuthenticator 8.0	8.0.2	Upgrade to 8.0.3 or above
FortiAuthenticator 8.0	8.0.0	Upgrade to 8.0.3 or above
FortiAuthenticator 6.6	6.6.0 through 6.6.8	Upgrade to 6.6.9 or above
FortiAuthenticator 6.5	6.5.0 through 6.5.6	Upgrade to 6.5.7 or above

3. FortiSandbox

Vulnerability Details

- **CVE ID:** CVE-2026-26083
- **IR Number:** FG-IR-26-136
- **Severity:** Critical
- **CVSS v3 Score:** 9.1
- **CWE: CWE-862 –** Missing Authorization
- A missing authorization vulnerability [CWE-862] in FortiSandbox, FortiSandbox Cloud and FortiSandbox PaaS WEB UI may allow an unauthenticated attacker to execute unauthorized code or commands via HTTP requests.

Version	Affected	Solution
FortiSandbox 5.0	5.0.0 through 5.0.1	Upgrade to 5.0.2 or above
FortiSandbox 4.4	4.4.0 through 4.4.8	Upgrade to 4.4.9 or above
FortiSandbox Cloud 24	All versions	Migrate to a fixed release
FortiSandbox Cloud 23	All versions	Migrate to a fixed release
FortiSandbox Cloud 5.0	5.0.2 through 5.0.5	Upgrade to 5.0.6 or above
FortiSandbox PaaS 23.4	23.4 all versions	Migrate to a fixed release
FortiSandbox PaaS 23.3	23.3 all versions	Migrate to a fixed release
FortiSandbox PaaS 23.1	23.1 all versions	Migrate to a fixed release
FortiSandbox PaaS 22.2	22.2 all versions	Migrate to a fixed release
FortiSandbox PaaS 22.1	22.1 all versions	Migrate to a fixed release
FortiSandbox PaaS 21.4	21.4 all versions	Migrate to a fixed release
FortiSandbox PaaS 21.3	21.3 all versions	Migrate to a fixed release
FortiSandbox PaaS 5.0	5.0.0 through 5.0.1	Upgrade to 5.0.2 or above
FortiSandbox PaaS 4.4	4.4.5 through 4.4.8	Upgrade to 4.4.9 or above

RECOMMENDATIONS:

Immediate Actions

- Upgrade all affected Fortinet products to the latest fixed releases immediately.
- Prioritize internet-facing FortiAuthenticator and FortiSandbox deployments.

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-26-136
- https://fortiguard.fortinet.com/psirt/FG-IR-26-128
- https://fortiguard.fortinet.com/psirt/FG-IR-26-123