مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Fortinet December 2025 Security Update

Tracking #:432318117

Date:10-12-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Fortinet has released a series of security updates addressing two critical-severity vulnerabilities and multiple high-severity vulnerabilities across several product lines, including FortiVoice, FortiSandbox, FortiWeb, FortiOS, FortiProxy, and FortiSwitchManager.

TECHNICAL DETAILS:

Fortinet has released a series of security updates addressing multiple high-severity and two critical-severity vulnerabilities across several product lines, including FortiVoice, FortiSandbox, FortiWeb, FortiOS, FortiProxy, and FortiSwitchManager. The latest disclosures include critical improper access control flaws (CVE-2025-59718, CVE-2025-59719) that may allow unauthorized administrative access. Additional vulnerabilities span path traversal, OS command injection, authentication cookie forgery, and FortiCloud SSO authentication bypass issues.

Critical Vulnerability Details:

1. **CVE IDs: CVE-2025-59718, CVE-2025-59719**
   - Severity: Critical
   - CVSSv3: 9.1
   - Impact: Improper Access Control (Potential Full Administrative Compromise)
   - An Improper Verification of Cryptographic Signature vulnerability [CWE-347] in FortiOS, FortiWeb, FortiProxy and FortiSwitchManager may allow an unauthenticated attacker to bypass the FortiCloud SSO login authentication via a crafted SAML message, if that feature is enabled on the device.
   - The FortiCloud SSO login feature is not enabled in default factory settings. However, when an administrator registers the device to FortiCare from the device's GUI, unless the administrator disables the toggle switch "Allow administrative login using FortiCloud SSO" in the registration page, FortiCloud SSO login is enabled upon registration.

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
FortiOS 7.0	7.0.0 through 7.0.17	Upgrade to 7.0.18 or above
FortiOS 6.4	Not affected	Not Applicable
FortiProxy 7.6	7.6.0 through 7.6.3	Upgrade to 7.6.4 or above
FortiProxy 7.4	7.4.0 through 7.4.10	Upgrade to 7.4.11 or above
FortiProxy 7.2	7.2.0 through 7.2.14	Upgrade to 7.2.15 or above
FortiProxy 7.0	7.0.0 through 7.0.21	Upgrade to 7.0.22 or above
FortiSwitchManager 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiSwitchManager 7.0	7.0.0 through 7.0.5	Upgrade to 7.0.6 or above
FortiWeb 8.0	8.0.0	Upgrade to 8.0.1 or above
FortiWeb 7.6	7.6.0 through 7.6.4	Upgrade to 7.6.5 or above
FortiWeb 7.4	7.4.0 through 7.4.9	Upgrade to 7.4.10 or above
FortiWeb 7.2	Not affected	Not Applicable
FortiWeb 7.0	Not affected	Not Applicable

High Severity Vulnerabilities:

1. Path Traversal in FortiVoice (CVE-2025-60024)
   - Severity: High (CVSS 7.7)
   - Impact: Arbitrary File Write, Privilege Escalation

Version	Affected	Solution
FortiVoice 7.2	7.2.0 through 7.2.2	Upgrade to 7.2.3 or above
FortiVoice 7.0	7.0.0 through 7.0.7	Upgrade to 7.0.8 or above

2. OS Command Injection in FortiSandbox (CVE-2025-53949)
   - Severity: High (CVSS 7.0)
   - Impact: Unauthorized Command Execution

Version	Affected	Solution
FortiSandbox 5.0	5.0.0 through 5.0.2	Upgrade to 5.0.3 or above
FortiSandbox 4.4	4.4.0 through 4.4.7	Upgrade to 4.4.8 or above
FortiSandbox 4.2	4.2 all versions	Migrate to a fixed release
FortiSandbox 4.0	4.0 all versions	Migrate to a fixed release

3. Authentication Cookie Forgery in FortiWeb (CVE-2025-64447)
   - Severity: High (CVSS 7.1)
   - Impact: Privilege Escalation via Forged Cookies

Version	Affected	Solution
FortiWeb 8.0	8.0.0 through 8.0.1	Upgrade to 8.0.2 or above
FortiWeb 7.6	7.6.0 through 7.6.5	Upgrade to 7.6.6 or above
FortiWeb 7.4	7.4.0 through 7.4.10	Upgrade to 7.4.11 or above
FortiWeb 7.2	7.2.0 through 7.2.11	Upgrade to 7.2.12 or above
FortiWeb 7.0	7.0.0 through 7.0.11	Upgrade to 7.0.12 or above

RECOMMENDATIONS:

- Apply security updates immediately, prioritizing the critical improper access control vulnerabilities
- Upgrade all affected products to the vendor-recommended fixed versions, beginning with all systems exposed to administrative access or reachable from external or untrusted networks.
- Disable FortiCloud SSO login on FortiOS, FortiWeb, FortiProxy, and FortiSwitchManager devices until they are fully upgraded, as this feature is directly affected by an authentication bypass vulnerability.

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-25-647
- https://fortiguard.fortinet.com/psirt/FG-IR-25-479
- https://fortiguard.fortinet.com/psirt/FG-IR-25-812
- https://fortiguard.fortinet.com/psirt/FG-IR-25-945