EnCyb

Severity: Critical

Advisory Type: Security

Critical Vulnerabilities Identified in Fortinet Products

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Two critical Fortinet vulnerabilities (CVE-2025-59718 and CVE-2025-59719) allow unauthenticated attackers to bypass FortiCloud SSO via improper SAML signature verification.

- CVE ID: CVE-2025-59718, CVE-2025-59719
- Active Region: Global
- Affected Sector: Any sector using Fortinet network/security infrastructure
- Affected Product: FortiOS, FortiProxy, FortiSwitchManager, FortiWeb
- Severity: Critical
- Published Date: December 09, 2025

TECHNICAL DETAILS

- Target: This vulnerability targets Fortinet devices that have FortiCloud SSO enabled, including FortiOS, FortiProxy, FortiSwitchManager, and FortiWeb systems. By exploiting the flaw, attackers can gain administrative access to critical network-security infrastructure and assume control over enforcement and management functions.
- Root Cause: The root cause is a failure to properly validate the cryptographic signature in SAML authentication responses, allowing forged assertions to pass as legitimate. This breakdown in signature verification undermines the integrity of the federated login process and enables unauthorized administrative access without credentials.
- Prerequistic For Exploitation: To exploit this vulnerability, the attacker must be able to reach the device's management interface and have FortiCloud SSO enabled on the target system. Because no valid credentials are required, the attacker only needs the capability to send a crafted SAML message that bypasses the flawed signature check.

AFFECTED VERSIONS TABLE

Product	Affected Versions	Remediation
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	None
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

IMPACT

- Unauthorized admin access to Fortinet devices.
- Ability to disable or alter security controls.
- Facilitates lateral movement across the network.
- Enables impersonation of trusted SSO identities.
- Increases risk of full infrastructure compromise.
- Can deploy malware or persistence mechanisms on management planes.

RECOMMENDATIONS

- Upgrade all affected Fortinet products to the fixed versions immediately.
- Disable FortiCloud SSO on all devices until updates are applied.
- Limit management access to trusted networks with strict ACLs.
- Verify no unauthorized admin accounts or config changes exist post-patch.
- Enforce MFA and strengthen identity controls on all admin interfaces.
- Review logs for unusual SAML activity or suspicious admin actions.

REFRENCE

- https://fortiguard.fortinet.com/psirt/FG-IR-25-647
- https://cybersecuritynews.com/critical-fortinet-vulnerability/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb soc@encyb.com

www.encyb.com