Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Fortinet Authentication Bug Sparks Rapid Exploitation

Date of Publication	Admiralty Code	TA Number
December 18, 2025	A1	TA2025382

Summary

First Seen: December 9, 2025
Affected Products: FortiOS, FortiProxy, FortiSwitchManager, FortiWeb
Impact: Threat actors are actively exploiting two critical Fortinet vulnerabilities, CVE-2025-59718 and CVE-2025-59719, enabling unauthenticated bypass of FortiCloud SSO authentication through crafted SAML responses. Exploitation began within days of disclosure and targets FortiGate and related Fortinet products, where FortiCloud SSO was unintentionally enabled during FortiCare registration. Attackers gain administrative access, exfiltrate device configurations, and potentially compromise hashed credentials. Organizations should immediately patch affected systems, disable FortiCloud SSO, and restrict administrative access to mitigate ongoing risk.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-59718	Fortinet Multiple Products Improper Verification of Cryptographic Signature Vulnerability	Fortinet FortiOS, FortiProxy, FortiSwitchManager	✗	✓	✓
CVE-2025-59719	Fortinet FortiCloud SSO Login Authentication Bypass	Fortinet FortiWeb	✗	✗	✓

Vulnerability Details

#1 Threat actors moved rapidly to weaponize two newly disclosed Fortinet vulnerabilities, exploiting them less than a day after public disclosure. Tracked as CVE-2025-59718 and CVE-2025-59719, these critical flaws enable unauthenticated remote attackers to bypass FortiCloud Single Sign-On (SSO) authentication by submitting crafted SAML response messages.

#2 The root cause is improper verification of cryptographic signatures within the FortiCloud SSO login mechanism. Affected products span multiple enterprise platforms, including FortiOS, FortiProxy, FortiSwitchManager, and FortiWeb across several version branches.

#3 Although FortiCloud SSO is disabled by default, risk emerges during device registration. When administrators enroll devices with FortiCare through the graphical interface, FortiCloud SSO is automatically enabled unless the "Allow administrative login using FortiCloud SSO" option is explicitly disabled. This silent enablement creates an unexpected exposure surface.

#4 Active exploitation was confirmed beginning December 12, 2025, just three days after disclosure. Observed attacks focused on abusing SSO authentication to gain access to FortiGate appliances, typically targeting the "admin" account. Following access, attackers exfiltrated full device configurations. While stored credentials are hashed, offline cracking remains feasible, particularly against weak or reused passwords. Any organization observing related malicious activity should treat all extracted credentials as compromised and reset them immediately.

#5 Given Fortinet's long-standing attractiveness as an initial access vector, continued **exploitation** is expected. Organizations running affected versions should apply patches without delay. Until remediation is complete, FortiCloud SSO login should be disabled, and administrative access to firewall and VPN management interfaces should be strictly restricted to trusted internal networks.

Vulnerabilities

CVE ID	AFFECTED PRODUCT	AFFECTED CPE	CWE ID
CVE-2025-59718	Fortinet Fortios Before 7.0.18, Before 7.2.12, Before 7.4.9, Before 7.6.4; Fortinet Fortiproxy Before 7.0.22, Before 7.2.15, Before 7.4.11, Before 7.6.4; Fortinet Fortiswitchmanager Before 7.0.6, Before 7.2.7	cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiswitchmanager:*:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	CWE-347
CVE-2025-59719	Fortinet Fortiweb Before 7.4.10, Before 7.6.5, Before 8.0.1	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*	CWE-347

Recommendations

Disable FortiCloud SSO Immediately: FortiCloud SSO is disabled by default but may be unintentionally enabled during FortiCare registration. Disable the "Allow administrative login using FortiCloud SSO" setting on all vulnerable devices until upgrades are completed. Use the GUI or CLI to ensure the feature is fully disabled across all affected products.

Apply Security Patches Without Delay: Upgrade to non-affected Fortinet versions as soon as patches are available. Do not re-enable FortiCloud SSO until devices are confirmed to be running a fixed release. Prioritize internet-facing FortiGate and related appliances.

Monitor for Indicators of Compromise: Review logs for successful SSO-based admin logins from unfamiliar external IP addresses. Watch for configuration exports performed through the GUI shortly after authentication events. Treat any unexplained admin activity as potentially malicious.

Restrict Management Interface Exposure: Limit firewall and VPN management access to trusted internal networks only. Remove direct internet access to administrative interfaces wherever possible. Enforce network segmentation to reduce blast radius in the event of compromise.

Harden Administrative Access Controls: Enforce strong password policies and minimize the use of shared administrative accounts. Regularly audit administrative privileges and remove unnecessary access. Treat firewall and VPN appliances as high-value assets requiring elevated protection.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0009 Collection	TA0011 Command and Control	T1190 Exploit Public-Facing Application	T1078 Valid Accounts

T1133 External Remote Services	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools	**T1530** Data from Cloud Storage
T1005 Data from Local System	**T1071** Application Layer Protocol	**T1071.001** Web Protocols	**T1556** Modify Authentication Process

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	45[.]32[.]153[.]218, 167[.]179[.]76[.]111, 199[.]247[.]7[.]82, 45[.]61[.]136[.]7, 38[.]54[.]88[.]203, 38[.]54[.]95[.]226, 38[.]60[.]212[.]97

Patch Link

https://www.fortiguard.com/psirt/FG-IR-25-647

References

https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-sso-logins-following-disclosure-cve-2025-59718-cve-2025-59719/

https://arcticwolf.com/resources/blog/cve-2025-59718-and-cve-2025-59719/

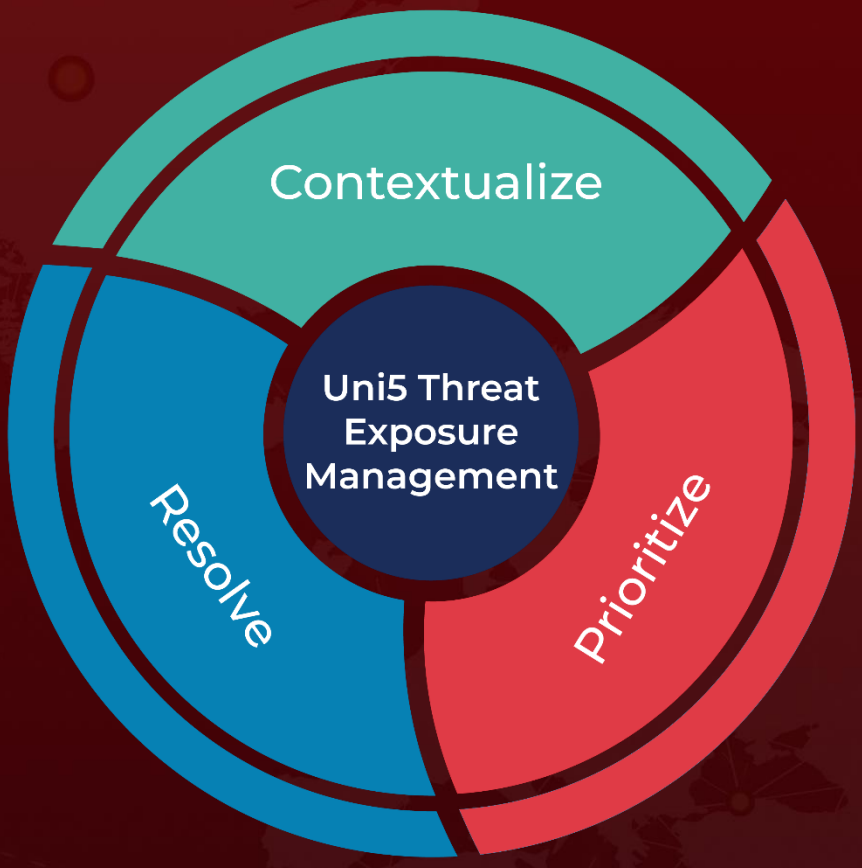
https://docs.fortinet.com/upgrade-tool

https://hivepro.com/threat-advisory/fortiweb-flaw-exploited-in-the-wild-patch-immediately/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 18, 2025 • 03:30 AM

More at www.hivepro.com