Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-24858: Critical FortiCloud SSO Zero-day Under Active Exploitation

Date of Publication	Admiralty Code	TA Number
January 28, 2026	A1	TA2026027

Summary

First Seen: January 15, 2026
Affected Products: Fortinet FortiOS, FortiManager, FortiAnalyzer, FortiProxy
Impact: CVE-2026-24858 is a critical authentication bypass vulnerability (CVSS 9.8) affecting multiple Fortinet products, including FortiOS, FortiManager, FortiAnalyzer, and FortiProxy, when FortiCloud Single Sign-On (SSO) is enabled. The flaw allows attackers with any valid FortiCloud account to gain unauthorized administrative access to devices belonging to other organizations, and has been actively exploited in the wild since mid-January 2026. Successful exploitation can lead to full device compromise, configuration tampering, and loss of control over perimeter security infrastructure. Immediate patching, disabling FortiCloud SSO where possible, and auditing for unauthorized administrative activity are strongly recommended.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-24858	Fortinet Multiple Products Authentication Bypass Using an Alternate Path or Channel Vulnerability	Fortinet FortiOS, FortiManager, FortiAnalyzer, FortiProxy	✓	✓	✓

Vulnerability Details

#1 CVE-2026-24858 is a critical authentication bypass vulnerability (CWE-288) with a CVSS score of 9.8, affecting Fortinet products including FortiOS, FortiManager, FortiAnalyzer, and FortiProxy when FortiCloud Single Sign-On (SSO) is enabled. FortiOS powers FortiGate firewalls, widely deployed enterprise-grade security appliances used for perimeter defense, VPN termination, and threat protection, while FortiManager and FortiAnalyzer provide centralized management and logging across Fortinet environments. Initial activity was suspected to be a patch bypass of CVE-2025-59718, but Fortinet confirmed this as a distinct vulnerability on January 23, 2026.

#2 The flaw stems from improper access control in the FortiCloud SSO trust mechanism, enabling authentication bypass via an alternate path. An attacker with any valid FortiCloud account and a registered device can exploit this weakness to authenticate to Fortinet devices belonging to other customers or organizations. Although FortiCloud SSO is disabled by default, it may be automatically enabled when devices are registered with FortiCare via the GUI, significantly expanding the exposed attack surface.

#3 Active exploitation has been observed since January 15, 2026, with threat actors using known malicious FortiCloud accounts to conduct automated attacks from Cloudflare-protected IP infrastructure. Post-exploitation activity includes downloading firewall configuration files, creating persistent local administrator accounts (e.g., secadmin, itadmin, support, backup), and modifying configurations to enable VPN access. This activity impacts multiple major product branches, particularly versions 7.0.x through 7.6.x, and poses severe risks including network compromise, lateral movement, and loss of control over critical security infrastructure, especially in environments heavily reliant on FortiCloud-based management.

#4 Fortinet has released FortiOS 7.4.11 to address this vulnerability, with patches for other affected branches forthcoming. Organizations should upgrade immediately, audit for unauthorized administrator accounts and suspicious FortiCloud authentication activity, and disable FortiCloud SSO on internet-facing devices until patching is complete.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-24858	Fortinet FortiOS (Before 7.0.19, 7.2.13, 7.4.11, 7.6.6) Fortinet FortiManager (Before 7.0.16, 7.2.13, 7.4.10, 7.6.6) Fortinet FortiAnalyzer (Before 7.0.16, 7.2.12, 7.4.10, 7.6.6) Fortinet FortiProxy (7.0, 7.2, Before 7.4.13, 7.6.6)	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortimanager:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortianalyzer:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*	CWE-288

Recommendations

Upgrade to Patched Firmware Versions: Upgrade all affected Fortinet devices to the latest firmware versions as soon as patches become available. Fortinet has announced upcoming releases including FortiOS 7.6.6, 7.2.13, and 7.0.19, as well as corresponding updates for FortiManager, FortiAnalyzer, and FortiProxy. Monitor official Fortinet channels and the FortiGuard PSIRT advisory for patch availability and follow the recommended upgrade path using the Fortinet upgrade tool at https://docs.fortinet.com/upgrade-tool.

Verify FortiCloud SSO Status: Although Fortinet has disabled FortiCloud SSO for vulnerable devices at the cloud level, administrators should verify the configuration on their devices. Navigate to System, then Settings, and ensure the "Allow administrative login using FortiCloud SSO" toggle is set to Off. Alternatively, use the CLI command config system global and set sso-enabled disable.

Audit Administrator Accounts: Conduct an immediate audit of all administrator accounts on affected devices. Look specifically for unauthorized accounts with names such as audit, backup, itadmin, secadmin, support, backupadmin, deploy, remoteadmin, security, svcadmin, or system. Remove any accounts that were not created by authorized personnel and reset passwords for all legitimate administrative accounts.

Review Authentication Logs: Examine device authentication logs for any logins from the known malicious accounts cloud-noc[@]mail[.]io and cloud-init[@]mail[.]io. Also search for authentication attempts from the identified threat actor IP addresses.

Restore Clean Configuration: If compromise indicators are detected, treat the device as fully compromised. Restore the configuration from a known clean backup taken before January 2026, or conduct a thorough manual audit of all configuration changes. Pay particular attention to VPN configurations, firewall policies, and administrative access settings.

Rotate Connected Credentials: Change all credentials for LDAP and Active Directory accounts that may be connected to or accessible from the FortiGate devices. Attackers who exfiltrated configurations may have obtained stored credentials or service account information that could be used for lateral movement.

Implement Network Segmentation: Restrict administrative access to Fortinet devices to dedicated management networks only. Ensure that management interfaces are not exposed directly to the internet and require VPN or jump host access for remote administration.

Establish Continuous Monitoring: Implement enhanced monitoring for any new administrator account creation, configuration changes, and unusual authentication patterns on all Fortinet devices. Configure alerts for logins from unexpected geographic locations or during non-business hours.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1136: Create Account	T1136.001: Local Account
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Collection	T1005: Data from Local System	
Command and Control	T1090: Proxy	T1090.002: External Proxy
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits

Indicators of Compromise (IOCs)

TYPE	VALUE
Email Address	cloud-noc[@]mail[.]io, cloud-init[@]mail[.]io
IPv4	104[.]28[.]244[.]115, 104[.]28[.]212[.]114, 104[.]28[.]212[.]115, 104[.]28[.]195[.]105, 104[.]28[.]195[.]106, 104[.]28[.]227[.]106, 104[.]28[.]227[.]105, 104[.]28[.]244[.]114, 37[.]1[.]209[.]19, 217[.]119[.]139[.]50
Local Admin Account	audit, backup, itadmin, secadmin, support, backupadmin, deploy, itadmin, remoteadmin, security, svcadmin, system

Patch Details

- Fortinet has released patches for the 7.4 branch: FortiOS 7.4.11, FortiManager 7.4.10, and FortiAnalyzer 7.4.10.
- Patches for other branches are upcoming: FortiOS (7.0.19, 7.2.13, 7.6.6), FortiManager (7.0.16, 7.2.13, 7.6.6), FortiAnalyzer (7.0.16, 7.2.12, 7.6.6), and FortiProxy (7.4.13, 7.6.6).
- FortiProxy 7.0.x and 7.2.x users must migrate to a supported fixed release as no patches will be provided.
- FortiOS 6.4, FortiManager 6.4, and FortiAnalyzer 6.4 are not affected.

Links:
https://fortiguard.fortinet.com/psirt/FG-IR-26-060
https://docs.fortinet.com/upgrade-tool

References

https://fortiguard.fortinet.com/psirt/FG-IR-26-060

https://www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios

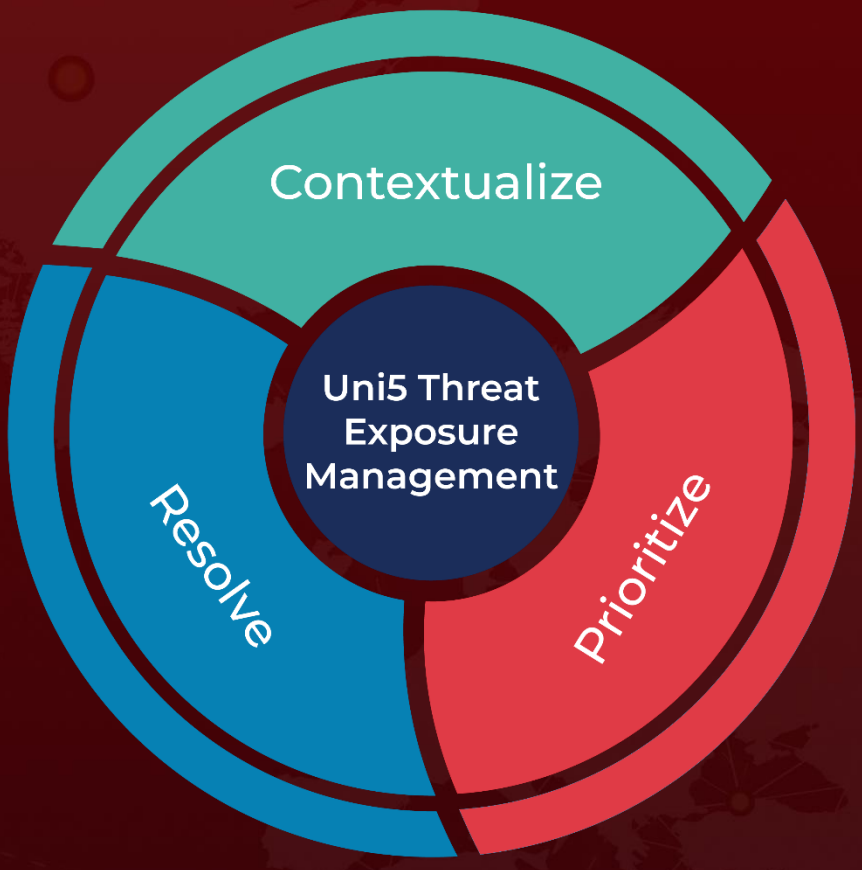
https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-configuration-changes-fortinet-fortigate-devices-via-sso-accounts/

https://hivepro.com/threat-advisory/fortinet-authentication-bug-sparks-rapid-exploitation/

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

January 28, 2026 • 09:00 AM

More at www.hivepro.com