Fortinet Confirms Active Exploitation of FortiCloud SSO Auth Bypass

TL;DR

Attackers are exploiting a FortiCloud SSO authentication bypass vulnerability, tracked as CVE-2026-24858, to gain unauthorized administrative access to Fortinet devices where FortiCloud SSO is enabled.

Fortinet temporarily disabled SSO to contain the activity and has re-enabled it with version enforcement.

Overview

Fortinet confirmed active exploitation of an authentication bypass vulnerability affecting FortiCloud Single Sign-On (SSO), tracked as CVE-2026-24858 (CVSS 9.4). The flaw allows attackers with a FortiCloud account and a registered device to authenticate to other customers' devices when FortiCloud SSO is enabled. While FortiCloud SSO is not enabled by default, it can be activated during device registration unless administrators explicitly disable the option.

Fortinet identified malicious activity tied to two FortiCloud accounts and locked them on January 22, 2026. To stop further abuse, Fortinet disabled FortiCloud SSO on January 26 and re-enabled it on January 27 with controls that block logins from vulnerable versions. Devices running affected software must now be upgraded for FortiCloud SSO authentication to function.

Impacted Products

The following products are impacted **only when FortiCloud SSO is enabled**:

- FortiOS
- FortiManager
- FortiAnalyzer
- FortiProxy
- FortiWeb

Not impacted:

- FortiGate Cloud
- FortiManager Cloud
- FortiAnalyzer Cloud
- Deployments using a custom SSO Identity Provider, including FortiAuthenticator

Note: FortiSwitch Manager remains under investigation.

CVE-2026-24858 involves improper access control within the FortiCloud SSO authentication flow. After authentication, affected systems did not consistently enforce account-to-device restrictions, allowing administrative actions beyond the intended scope.

If exploited, CVE-2026-24858 gives an attacker admin-level access to Fortinet devices and visibility into how the network is configured. From there, they can add their own admin accounts, keep access over time, and use the device as a foothold to interfere with traffic or move further into the environment.

Aspire Protects

- **Patch** – Upgrade all affected Fortinet products to the fixed versions required for FortiCloud SSO authentication. See Fortinet's advisory for more information.
- Review FortiCloud SSO administrative login activity, with attention to January 2026 access.
- Audit all local administrator accounts and remove any that are not expected or documented.
- Rotate credentials tied to administrative access if unauthorized activity is identified.
- Consider disabling FortiCloud SSO in environments where patching cannot be completed immediately.

TTPs

Initial Access

- Valid Accounts [T1078] – The attacker may have authenticated to Fortinet devices using FortiCloud SSO credentials to gain administrative access without local authentication.

Persistence

- Create Account [T1136] – The attacker may have added new local administrator accounts to maintain access after the initial login.

Collection

- Data from Configuration Repository [T1602] – The attacker may have downloaded device configuration files after gaining administrative access.

IoCs

FortiCloud SSO Accounts

- cloud-noc[@]mail[.]io
- cloud-init[@]mail[.]io

IP Addresses

- 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 Administrator Account Names

- audit
- backup
- backupadmin
- deploy
- itadmin
- remoteadmin
- secadmin
- security
- support
- svcadmin
- system

Targeted Industries

Fortinet devices with FortiCloud SSO enabled are commonly used to manage core network and security functions, which makes organizations in the following industries more likely to be affected by this activity:

- Government
- Education
- Healthcare
- Finance
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

PSIRT | FortiGuard Labs
Analysis of Single Sign-On Abuse on FortiOS | Fortinet Blog