UPDATE: Fortinet FortiCloud SSO Authentication Bypass Allows Unauthorized Administrative Access

TL;DR

Two authentication bypass vulnerabilities in FortiCloud SSO (CVE-2025-59718 and CVE-2025-59719) let an attacker slip past login checks with a forged SAML message.

The feature is off by default but quietly turns on during FortiCare registration unless the admin disables the toggle. FortiCloud SSO should be turned off and updated as soon as possible.

Update - 1/23/2026

In December 2025, Aspire's CTI team issued an Emergency Flash Notice addressing two bypass vulnerabilities (CVE-2025-59718 and CVE-2025-59719) in FortiCloud SSO. This month, multiple security firms confirmed active, automated exploitation against Fortinet FortiGate devices with FortiCloud SSO enabled. Exploitation began around January 15. Attackers were able to create admin and VPN accounts and export **firewall configurations** almost instantly.

The Issue

FortiOS 7.4.10 does not fully fix CVE-2025-59718. Customers have reported successful compromises on systems running that version. Fortinet stated that the issue was not fully resolved and plans to release additional updates, including FortiOS 7.4.11, 7.6.6, and 8.0.0, to address the remaining gap.

Observed activity closely mirrors exploitation documented in December 2025. This includes SSO logins associated with the email address **cloud-init@mail[.]io** and the source IP **104[.]28[.]244[.]114**, which was previously tied to FortiCloud SSO abuse. As of this update, Shadowserver is tracking nearly 11,000 internet-exposed Fortinet devices with FortiCloud SSO still enabled, increasing the attack surface.

Until Fortinet releases and customers apply the future fixes, **disabling FortiCloud SSO** remains the most reliable defensive measure, even on systems believed to be fully patched. This update applies only to CVE-2025-59718. CVE-2025-59719 is not part of the current activity.

Overview

Fortinet addressed vulnerabilities (CVE 2025-59718 and CVE-2025-59719, CVSS 9.8) in FortiOS, FortiWeb, FortiProxy, and FortiSwitchManager that allow an attacker to bypass FortiCloud SSO authentication without valid credentials. Both flaws stem from weak signature checks in SAML messages processed during FortiCloud login and a forged SAML message is enough to grant administrative access when the feature is turned on.

If either vulnerability is exploited, an attacker can enter the admin console, alter configurations, weaken firewall rules, create new accounts, remove logging, or set up deeper access across the network. There is no password challenge involved. The only condition is that FortiCloud SSO is active.

Affected Products

- CVE 2025-59718
  - FortiOS
  - FortiProxy
  - FortiSwitchManager
- CVE-2025-59719
  - FortiWeb

***Note**: See which versions are impacted for CVE-2025-59718 and CVE-2025-59719 in Fortinet's advisory.*

The problem for many organizations is that FortiCloud SSO is not on by default, but it becomes active during FortiCare registration, and it only turns off if the admin notices the toggle and switches it off.

CVE 2025 59808 and CVE 2025 64471, CVSS 7.5

Fortinet also fixed two related account security issues. One vulnerability lets someone who has already accessed an account reset the password without entering the current one (CVE-2025 59808, CVSS 6.8). Another accepts a password hash instead of the real password (CVE 2025 64471, CVSS 7.5). These problems make account takeover easier once an attacker is inside the network.

Affected Products

- CVE 2025 59808
  - FortiSOAR

- CVE 2025 64471
  - FortiWeb

***Note**: See which versions are impacted in Fortinet's advisory for CVE-2025-64471 and CVE-2025-59808.*

Attackers have a long history of targeting Fortinet appliances, from ransomware groups to state-backed operators. These vulnerabilities create a single-entry point that gives them the kind of administrative access they try to gain during early intrusion stages. Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch** – For CVE-2025-59718 and CVE-2025-59719, update to a fixed version using Fortinet's upgrade tool.
  - Review recent administrative activity for unexpected logins.
  - Confirm whether FortiCloud SSO was automatically enabled during FortiCare registration and correct it as needed.
- Turn off FortiCloud SSO login on every device where it is active. In the GUI, go to System, then Settings, and switch off "Allow administrative login using FortiCloud SSO." In the CLI, use the following commands:
  - ```
    config system global
    set admin-forticloud-sso-login disable
    end
    ```
- **Patch** – For CVE-2025-59808 and CVE-2025-64471, update FortiSOAR and FortiWeb to the fixed versions listed in Fortinet's advisories.
- Review all user accounts for unauthorized password resets.
- Enforce MFA across administrative and user accounts.
- Check authentication logs for unexpected login behavior or password hash based logins.

TTPs to Watch

CVE-2025-59718 and CVE-2025-59719

- Credential Access
  - Use Alternate Authentication Material [T1550] – The attacker may have supplied a forged SAML message to bypass FortiCloud SSO and enter the administrative interface without valid credentials.
- Credential Access
    ```

- Valid Accounts [T1078] – The attacker may have impersonated a trusted FortiCloud user by presenting crafted authentication data that the device accepted as legitimate.

CVE 2025 59808 and CVE 2025 64471

- Credential Access
  - Account Manipulation [T1098] – The attacker may have reset account credentials or authenticated with password hashes, allowing unauthorized access to user accounts without providing the original password.
- Credential Access
  - Use Alternate Authentication Material [T1550] – The attacker may have authenticated with non-standard authentication material, such as a password hash, instead of the real password.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Any organization running affected Fortinet products with FortiCloud SSO enabled could be exposed.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance
- Technology
- Legal
- 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

CVE-2025-59718 and CVE-2025-59719 | Arctic Wolf
PSIRT | FortiGuard Labs
PSIRT | FortiGuard Labs
PSIRT | FortiGuard Labs
Fortinet Document Library | Upgrade Path Tool