Enemy at the FortiGates: Fortinet Devices Remain Vulnerable to SSO Authentication Bypass

Summary

Starting 15 January 2026, security researchers at Arctic Wolf identified the compromise of fully-patched Fortinet FortiGate devices where attackers likely exploited the FortiCloud single sign-on (SSO) service.[1]

On 22 January 2026, Fortinet acknowledged there is an active security issue with FortiCloud SSO that was not addressed in the December 2025 security patches for vulnerabilities CVE-2025-59718 and CVE-2025-59719. Fortinet urges customers to implement mitigations against this attack as a security patch is not available at the time of publication.[2]

Details

On 9 December 2025, Fortinet released patches to address two critical vulnerabilities (CVE-2025-59718 and CVE-2025-59719) affecting FortiOS (used by FortiGate), FortiWeb, FortiProxy, and FortiSwitchManager.[3] The vulnerabilities were in FortiCloud's SSO service where an attacker could bypass authentication by sending a specially-crafted SAML request to gain administrative access.

Since 15 January 2026, Arctic Wolf observed malicious SSO authentications from accounts `cloud-init@mail.io` and `cloud-noc@mail.io` to FortiGate devices. After successful compromise, attackers created additional accounts for persistence and exfiltrated firewall configuration files. The authentications originated from IPs provided by the hosting providers Cloudflare (AS13335), Galeon (AS209290), and HVC (AS29802). CSIRT Italy also corroborated this renewed exploitation activity.[4]

On 22 January 2026, Fortinet's security team (PSIRT) published an initial analysis of the security incidents reported by Arctic Wolf, noting "the exploit was to a device that had been fully upgraded to the latest release at the time of the attack, which suggested a new attack path."

At the time of publication, there is neither an available security patch nor published CVE for Fortinet products affected by this new FortiCloud SSO vulnerability. Instead, Fortinet recommends implementing mitigations to disable FortiCloud SSO and further restrict administrative console access to internal networks.

CyberAlberta Threat Intelligence identified Fortinet assets in Alberta, although it is not clear what versions are installed or if the FortiCloud SSO login feature is enabled.

---

[1] https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-configuration-changes-fortinet-fortigate-devices-via-sso-accounts/
[2] https://www.fortinet.com/blog/psirt-blogs/analysis-of-sso-abuse-on-fortios
[3] https://fortiguard.fortinet.com/psirt/FG-IR-25-647
[4] https://www.acn.gov.it/portale/w/rilevato-possibile-sfruttamento-attivo-di-vulnerabilita-gia-note-in-prodotti-fortinet

Assessment

CyberAlberta Threat Intelligence assesses it is likely that all versions of Fortinet products with the FortiCloud SSO service enabled remain vulnerable to an authentication bypass. If the FortiCloud SSO service is enabled, check for indicators of compromise and implement Fortinet's recommended mitigations.

Recommendations

- Confirm if the FortiCloud SSO login feature is enabled, and disable if it is.
  - To disable, go to System > Settings > Set "Allow administrative login using FortiCloud SSO" to Off. Or input the following command in the CLI

```
config system global
set admin-forticloud-sso-login disable
end
```

- If FortiCloud SSO login feature is enabled and publicly accessible, investigate for signs of compromise including SAML requests from anomalous IPs, authentications with anomalous accounts such as `cloud-init@mail.io` and `cloud-noc@mail.io`, creation of new accounts and exfiltration of configuration data.
  - If any evidence of compromise is identified, then disable any new accounts and rotate credentials for legitimate accounts.
- Continue to monitor for updates from Fortinet regarding any new patches.
- Restrict access to Fortinet management interfaces to trusted internal network ranges only.

Indicators of Compromise (IOCs)

The following IOCs are provided by Arctic Wolf to help identify evidence of exploitation:

Description	IOC
Exploitation and exfiltration IPs	`104.28.244[.]115`
	`104.28.212[.]114`
	`217.119.139[.]50`
	`37.1.209[.]19`
Malicious account authentication	`cloud-init@mail.io`
	`cloud-noc@mail.io`
Maliciously-created local admin account	`secadmin`
	`itadmin`
	`support`
	`backup`
	`remoteadmin`

	audit

Table 1 - IOCs provided by Arctic Wolf characterizing recent exploitation of FortiGate devices