Arctic Wolf Observes Malicious SSO Logins on FortiGate Devices Following Disclosure of CVE-2025-59718 and CVE-2025-59719

On December 12, 2025, Arctic Wolf began observing intrusions involving malicious SSO logins on FortiGate appliances.

December 15, 2025 | by Arctic Wolf Labs | Security Bulletins

9 min read

On December 12, 2025, Arctic Wolf began observing intrusions involving malicious SSO logins on FortiGate appliances. Fortinet had previously released an advisory for two critical authentication bypass vulnerabilities (CVE-2025-59718 and CVE-2025-59719) on December 9, 2025. Arctic Wolf had also sent out a security bulletin for the vulnerabilities shortly thereafter.

These vulnerabilities allow unauthenticated bypass of SSO login authentication via crafted SAML messages, if the FortiCloud SSO feature is enabled on affected Devices. Several product lines were reported to be affected, including FortiOS, FortiWeb, FortiProxy, and FortiSwitchManager.

In their recent advisory, Fortinet stated that FortiCloud SSO login is disabled by default in factory settings. However, when administrators register devices using FortiCare through the GUI, FortiCloud SSO is enabled upon registration unless the “Allow administrative login using FortiCloud SSO” setting is disabled on the registration page.

Technical Details

In recently observed intrusions, malicious SSO logins on FortiGate devices originated from a handful of hosting providers, listed in the table below.

IOC	Hosting Provider
45.32.153[.]218	The Constant Company llc
167.179.76[.]111	The Constant Company llc
199.247.7[.]82	The Constant Company llc
45.61.136[.]7	BI Networks
38.54.88[.]203	Kaopu Cloud Hk Limited
38.54.95[.]226	Kaopu Cloud Hk Limited

Malicious logins were typically against the `admin` account, as shown in the example log line below:


```
date=2025-12-12 time=REDACTED devname=REDACTED devid=REDACTED eventtime=REDACTED
tz=REDACTED logid="0100032001" type="event" subtype="system" level="information"
vd="root" logdesc="Admin login successful" sn=REDACTED user="admin"
ui="sso(199.247.7[.]82)" method="sso" srcip=199.247.7[.]82 dstip=REDACTED
action="login" status="success" reason="none" profile="super_admin"
msg="Administrator admin logged in successfully from sso(199.247.7[.]82)"
```

Following malicious SSO logins, configurations were exported to the same IP addresses via the GUI interface.

```
date=2025-12-12 time=REDACTED devname=REDACTED devid=REDACTED eventtime=REDACTED
tz=REDACTED logid="0100032095" type="event" subtype="system" level="warning"
vd="root" logdesc="Admin performed an action from GUI" user="admin"
ui="GUI(199.247.7[.]82)" action="download" status="success" msg="System config
file has been downloaded by user admin via GUI(199.247.7[.]82)"
```

Note: Arctic Wolf has detections in place to identify potential exploitation and will continue to alert customers if additional instances are identified.

Recommendations

Reset Firewall Credentials if Affected

Although credentials are typically hashed in network appliance configurations, threat actors are known to crack hashes offline, especially if credentials are weak and susceptible to dictionary attacks.

If you observe malicious activity similar to the malicious logs described in this security bulletin, assume that hashed firewall credentials stored in the exfiltrated configurations have been compromised, and reset those credentials as soon as possible.

Limit Access to Management Interfaces of Firewall and VPN Appliances to Trusted Internal Users

Threat actors commonly target management interfaces of firewalls and VPNs for mass exploitation, often relying on specialized search engines that facilitate identification of specific hardware configurations.

In the last few years, Arctic Wolf observed **multiple** campaigns targeting management interfaces on firewalls and VPN gateways. Consider restricting all firewall management interface access to trusted internal networks as a security best security practice across all firewall configurations, regardless of network appliance vendor.

Upgrade to Latest Fixed Version

Arctic Wolf **strongly recommends** that customers upgrade to the latest fixed version of affected Fortinet products.

Product	Affected Version	Fixed Version
FortiOS 7.6	7.6.0 through 7.6.3	7.6.4 or above

FortiOS 7.2	7.2.0 through 7.2.11	7.2.12 or above
FortiOS 7.0	7.0.0 through 7.0.17	7.0.18 or above
FortiProxy 7.6	7.6.0 through 7.6.3	7.6.4 or above
FortiProxy 7.4	7.4.0 through 7.4.10	7.4.11 or above
FortiProxy 7.2	7.2.0 through 7.2.14	7.2.15 or above
FortiProxy 7.0	7.0.0 through 7.0.21	7.0.22 or above
FortiSwitchManager 7.2	7.2.0 through 7.2.6	7.2.7 or above
FortiSwitchManager 7.0	7.0.0 through 7.0.5	7.0.6 or above
FortiWeb 8.0	8.0.0	8.0.1 or above
FortiWeb 7.6	7.6.0 through 7.6.4	7.6.5 or above
FortiWeb 7.4	7.4.0 through 7.4.9	7.4.10 or above

Note: The following products are unaffected by the vulnerabilities: FortiOS 6.4, FortiWeb 7.0, and FortiWeb 7.2.

Workaround

Fortinet recommends turning off the FortiCloud login feature (if enabled) temporarily until upgrading to a non-affected version.

To turn off FortiCloud login, go to System -> Settings -> Switch “Allow administrative login using FortiCloud SSO” to Off.

Or type the following command in the CLI:

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

References

- PSIRT Advisory
- Arctic Wolf Security Bulletin

What to read next

BACK TO BLOG →

REQUEST A DEMO

Security Bulletins

Update: Arctic Wolf Observes Threat Campaign Targeting BeyondTrust Remote...

February 13, 2026

VIEW POST →

Security Bulletins

Microsoft Patch Tuesday: February 2026

February 11, 2026

VIEW POST →

Security Bulletins

CVE-2026-21643: Critical SQL Injection in FortiClientEMS

February 9, 2026

VIEW POST →

Security Bulletins

CVE-2026-1731: Unauthenticated OS Command Injection Vulnerability in...

February 9, 2026

VIEW POST →