CYBER ADVISORY

Thursday, January 22, 2026 **CAL-CSIC-202601-A-009**

Update on Fortinet Authentication Bypass Vulnerabilities

Ineffective Vendor Patch | Continued Exploitation | Bypass Authentication | SSO Login

The California Cybersecurity Integration Center (Cal-CSIC) identified two critical vulnerabilities affecting multiple Fortinet products on 9 December 2025. CVE-2025-59718 and CVE-2025-59719 allows an unauthenticated attacker to bypass the FortiCloud SSO login authentication by submitting a crafted Security Assertion Markup Language (SAML) message.[1, 2]

Although Fortinet released a security advisory stating that the vulnerabilities were patched in FortiOS versions 7.6.4 and above, 7.4.9 and above, 7.2.12 and above, and 7.0.18 and above, active exploitation has continued nearly a month after disclosure, indicating an ineffective patch although a future patch is expected to be released.[3] Attackers are still able to obtain unauthorized access to admin accounts and steal system configuration files.

Additionally, both vulnerabilities have been exploited in the wild and added to CISA's Known Exploited Vulnerabilities (KEV) catalog. In recently observed intrusions, malicious SSO logins originated from a handful of hosting providers, listed in the Indicators of Compromise section below.[4]

Indicators of Compromise

IOC	Type
cloud-init@mail.io	Malicious account observed logging into firewall devices, downloading/exfiltrating a firewall config file
cloud-noc@mail.io	Malicious account observed logging into firewall devices, downloading/exfiltrating a firewall config file
104.28.244[.]115	Source IP observed in intrusions
104.28.212[.]114	Source IP observed in intrusions
217.119.139[.]50	Source IP observed in intrusions
37.1.209[.]19	Source IP observed in intrusions

secadmin	Account created following initial access
itadmin	Account created following initial access
support	Account created following initial access
backup	Account created following initial access
remoteadmin	Account created following initial access
audit	Account created following initial access

The Cal CSIC recommends to regularly check official channels for Fortinet advisories and product updates, and to follow the initial workaround outlined in the FortiGuard Advisory.[5]

References

[1] NVD; CVE-2025-59718 Detail; https://nvd.nist.gov/vuln/detail/CVE-2025-59718; accessed 21 January 2026.
[2] NVD; CVE-2025-59719 Detail; https://nvd.nist.gov/vuln/detail/CVE-2025-59719; accessed 21 January 2026.
[3] Help Net Security; Fully patched FortiGate firewalls are getting compromised via CVE-2025-59718? - Help Net Security; https://www.helpnetsecurity.com/2026/01/21/patched-fortigate-compromised-via-cve-2025-59718/; accessed 21 January 2026.
[4] Artic Wolf; Arctic Wolf Observes Malicious Configuration Changes On Fortinet FortiGate Devices via SSO Accounts; https://arcticwolf.com/resources/blog/arctic-wolf-observes-malicious-configuration-changes-fortinet-fortigate-devices-via-sso-accounts/; accessed 21 January 2026.
[5] PSIRT; Multiple Fortinet Products' FortiCloud SSO Login Authentication Bypass; https://fortiguard.fortinet.com/psirt/FG-IR-25-647; accessed 21 January 2026.