AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-59718

Authentifizierungs-Bypass über FortiCloud-SSO in Fortinet-Produkten.

Ein nicht authentifizierter Angreifer aus dem Internet kann mit einer gefälschten SAML-Nachricht die FortiCloud-SSO-Anmeldung umgehen und sich als Administrator anmelden – ohne Zugangsdaten. Beobachtete Angreifer laden unmittelbar die System-Konfiguration herunter, die gehashte Zugangsdaten enthält. Voraussetzung ist der aktivierte FortiCloud-SSO-Login; er wird bei der FortiCare-Registrierung eines Geräts stillschweigend eingeschaltet, sofern der Administrator ihn nicht ausdrücklich abschaltet.

> **Geschäftsrisiko:** vollständige Administrator-Übernahme der Firewall bzw. des Proxys – mit Potenzial für Abfluss aller Konfigurationsgeheimnisse, dauerhaften Fernzugriff und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,8 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz, ohne Rechte, ohne Zutun, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD-Basiswert 9,8; Fortinet nennt im Advisory einen zeitlich adjustierten Wert von 9,1.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
17. Dezember 2025	FortiOS & FortiProxy 7.0–7.6 FortiSwitchManager 7.0 / 7.2	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS 3.1 Basiswert (NVD)

Auth-Bypass
FortiCloud-SSO · admin-Zugriff

Aktiv
ausgenutzt · CISA KEV (16.12.2025)

SSO aktiv?
erst mit FortiCare-Registrierung

Die Ursache: Die betroffenen Geräte prüfen die kryptografische Signatur der SAML-Antwort des FortiCloud-Identity-Providers nicht ordnungsgemäß (CWE-347). Dadurch akzeptiert der SSO-Login-Dienst eine **gefälschte SAML-Nachricht** ohne gültige Signatur und meldet den Angreifer als vorhandenes Konto an – in der Praxis als `admin`. Angreifbar ist nur, wer den FortiCloud-SSO-Login aktiv hat; dieser wird bei der Geräte-Registrierung an FortiCare eingeschaltet, wenn der Schalter „Allow administrative login using FortiCloud SSO" nicht ausdrücklich deaktiviert wird.

ANGRIFFSKETTE

01
Gerät exponiert – FortiGate-/FortiProxy-Verwaltung ist aus dem Internet erreichbar, FortiCloud-SSO ist aktiv

02
SAML fälschen – manipulierte SAML-Antwort ohne gültige Signatur an den SSO-Login senden

03
SSO-Bypass – Anmeldung als bestehendes Konto (typisch admin) ohne Zugangsdaten

04
Konfig-Diebstahl – System-Konfiguration über die GUI exportiert – inklusive gehashter Zugangsdaten

Betroffenheit & Fixversionen

Produkt · Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.6	7.6.0 – 7.6.3	7.6.4
FortiOS 7.4	7.4.0 – 7.4.8	7.4.9
FortiOS 7.2	7.2.0 – 7.2.11	7.2.12
FortiOS 7.0	7.0.0 – 7.0.17	7.0.18
FortiProxy 7.6	7.6.0 – 7.6.3	7.6.4
FortiProxy 7.4	7.4.0 – 7.4.10	7.4.11
FortiProxy 7.2	7.2.0 – 7.2.14	7.2.15
FortiProxy 7.0	7.0.0 – 7.0.21	7.0.22
FortiSwitchManager 7.2	7.2.0 – 7.2.6	7.2.7
FortiSwitchManager 7.0	7.0.0 – 7.0.5	7.0.6
FortiWeb	eigene CVE-2025-59719	siehe Hinweis

Ihr Maßnahmenplan.

In dieser Reihenfolge – Mitigation vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

Produkt und Version gegen die Tabelle prüfen und feststellen, ob der FortiCloud-SSO-Login aktiv ist: GUI unter System → Settings bzw. per CLI. Nur ein aktivierter SSO-Login ist angreifbar.

```
get system global | grep admin-forticloud-sso-login
```

02 Sofort mitigieren (vor dem Patch)

FortiCloud-SSO-Login deaktivieren, solange er nicht zwingend benötigt wird. Von Fortinet als Behelf benannt:

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

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren – FortiOS `7.0.18` · `7.2.12` · `7.4.9` · `7.6.4`, FortiProxy `7.0.22` · `7.2.15` · `7.4.11` · `7.6.4`, FortiSwitchManager `7.0.6` · `7.2.7`.

04 Kompromittierung ausschließen

Auth-Logs auf erfolgreiche FortiCloud-SSO-Anmeldungen am admin-Konto aus unerwarteten Quell-IPs und auf anschließende Konfig-Downloads durchsuchen. Wurde eine Konfiguration exportiert, alle darin enthaltenen Geheimnisse (Passwörter, VPN-PSKs, API-Schlüssel, Zertifikate) als kompromittiert behandeln und rotieren. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 FortiWeb gesondert bewerten

Wird FortiWeb eingesetzt, die Schwester-CVE `CVE-2025-59719` separat einspielen (Fix ab `7.6.5` / `7.4.10` / `8.0.1`). Management-Interfaces grundsätzlich nicht offen ins Internet stellen.

Kompromittierungs-Indikatoren (IoCs)

AUTH-EREIGNIS

Erfolgreiche `FortiCloud SSO`-Anmeldung am `admin`-Konto aus unerwarteten Quell-IPs, ohne vorherige legitime SSO-Nutzung

FOLGEAKTIVITÄT

Unmittelbarer Export der System-Konfiguration über die GUI – enthält gehashte Zugangsdaten

KONFIG-MARKER

Neu angelegte Admin-Konten, geänderte Admin-Profile, unbekannte Trust-Host-/VPN-Einträge nach dem Login

Zur Einordnung: Fortinet und die Analysten haben keine stabilen Netz-IoCs (IPs/Hashes) veröffentlicht. Die Erkennung läuft über die Authentifizierungs-Logs und einen Abgleich der Gerätekonfiguration – kein Ersatz für die eigene Log-Analyse.

Wichtig: Erfolgreiche Angriffe erscheinen als reguläre FortiCloud-SSO-Anmeldung an einem gültigen admin-Konto – ohne Alarm. Wurde die Konfiguration exportiert, müssen sämtliche darin enthaltenen Zugangsdaten als offengelegt gelten und rotiert werden. Ohne kontinuierliche Auswertung der Auth-Logs bleibt ein bereits erfolgter Zugriff unsichtbar.

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

24/7-SOC aus München: Die FortiCloud-SSO-Admin-Anmeldung aus fremden Quellen und der unmittelbare Konfig-Export fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Internet erreichbare FortiGate-/FortiProxy-Verwaltungen mit aktivem FortiCloud-SSO-Login über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre FortiOS-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- FortiCloud-SSO-Login heute deaktivieren oder patchen – Management-Interface vom Internet trennen.
- Prüfen lassen, ob eine Konfiguration exportiert wurde; falls ja, alle Secrets rotieren und den Vorfall für eine etwaige Meldung dokumentieren.
- Über eine dauerhafte Überwachung des Perimeters entscheiden.

Ihr Part · unser Part. Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch vollständig in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2025-59718 und dem FortiOS-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-25-647 · NIST NVD CVE-2025-59718 · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 16.12.2025) · Rapid7 Emergent Threat Report. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.