AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-24858

Authentifizierungs-Bypass über Fortinet FortiCloud-SSO.

Ein Angreifer mit einem beliebigen FortiCloud-Konto und einem eigenen registrierten Gerät kann sich an fremden Fortinet-Geräten anmelden, sofern dort die FortiCloud-SSO-Anmeldung aktiviert ist – ohne Rechte auf dem Zielgerät. Die Lücke wurde als Zero-Day aktiv ausgenutzt; Fortinet sperrte zwei missbräuchliche Konten und schaltete FortiCloud-SSO Ende Januar 2026 zeitweise plattformweit ab.

> **Geschäftsrisiko:** unbefugter administrativer Zugriff auf Firewalls und Management-Systeme – mit Potenzial für dauerhafte Hintertüren, VPN-Zugänge für Fremde, Abfluss von Konfigurationen und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,4 / 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/E:H/RL:O/RC:C` – aus dem Netz, geringe Komplexität, ohne Rechte am Zielgerät, ohne Zutun – volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Fortinet weist 9,4 aus (temporaler Faktor: Exploit vorhanden, offizieller Fix); der NVD-Basiswert liegt bei 9,8.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Januar 2026 (Zero-Day)	FortiOS, FortiProxy, FortiManager, FortiAnalyzer, FortiWeb, FortiNAC-F, FortiSwitchManager – nur bei aktivem FortiCloud-SSO	Sofort

Das Wichtigste in 60 Sekunden.

9,4 · KRITISCH
CVSS-Schweregrad (Fortinet)

Auth-Bypass
FortiCloud-SSO über alternativen Kanal (CWE-288)

Zero-Day
aktiv ausgenutzt · CISA KEV (27.01.2026)

Nur bei SSO
FortiCloud-SSO muss aktiviert sein (kein Standard)

Die Ursache: Verwundbare Fortinet-Versionen prüfen bei der FortiCloud-SSO-Anmeldung nicht ausreichend, ob das anmeldende FortiCloud-Konto auch tatsächlich zum Zielgerät gehört (Authentication Bypass Using an Alternate Path or Channel, **CWE-288**). Wer irgendein FortiCloud-Konto mit einem selbst registrierten Gerät besitzt, kann sich dadurch an fremden Geräten anmelden, auf denen FortiCloud-SSO eingeschaltet ist – der Cloud-Vertrauenspfad wird zur Umgehung der lokalen Authentifizierung.

ANGRIFFSKETTE

01 **FortiCloud-Konto** – Angreifer legt ein (frei verfügbares) FortiCloud-Konto an und registriert ein eigenes Gerät

02 **Ziel mit SSO** – ein fremdes Gerät mit aktivierter FortiCloud-SSO-Anmeldung wird adressiert

03 **SSO-Bypass** – über den Cloud-Kanal erfolgt die Anmeldung ohne lokale Berechtigung am Zielgerät

04 **Persistenz** – lokale Admin-Konten anlegen, VPN-Zugänge einrichten, Konfiguration abziehen

Betroffenheit & Fixversionen

Fortinet-Produkt	Verwundbar bis	Fixversion (Ziel)
FortiOS	7.0.0–7.0.18 · 7.2.0–7.2.12 · 7.4.0–7.4.10 · 7.6.0–7.6.5	7.0.19 · 7.2.13 · 7.4.11 · 7.6.6
FortiProxy	7.0.0–7.0.22 · 7.2.0–7.2.15 · 7.4.0–7.4.12 · 7.6.0–7.6.4	7.0.23 · 7.2.16 · 7.4.13 · 7.6.5
FortiManager	7.0.0–7.0.15 · 7.2.0–7.2.11 · 7.4.0–7.4.9 · 7.6.0–7.6.5	7.0.16 · 7.2.12 · 7.4.10 · 7.6.6
FortiAnalyzer	7.0.0–7.0.15 · 7.2.0–7.2.11 · 7.4.0–7.4.9 · 7.6.0–7.6.5	7.0.16 · 7.2.12 · 7.4.10 · 7.6.6
FortiWeb	7.4.0–7.4.11 · 7.6.0–7.6.6 · 8.0.0–8.0.3	7.4.12 · 7.6.7 · 8.0.4
FortiNAC-F	7.6.3–7.6.5	7.6.6
FortiSwitchManager	7.0.0–7.0.7 · 7.2.0–7.2.8	7.0.8 · 7.2.9

Angreifbar nur, wenn **FortiCloud-SSO-Anmeldung aktiviert** ist (kein Werksstandard). Exakte Build-Ranges und Fixversionen des eigenen Zweigs gegen das Hersteller-Advisory FG-IR-26-060 abgleichen; FortiCloud-SSO lässt vorübergehend keine Anmeldung von verwundbaren Versionen mehr zu.

Regulatorischer Hinweis: Ein bestätigter unbefugter administrativer Zugriff kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen, wir unterstützen bei Bewertung und Dokumentation.

Ihr Maßnahmenplan.

In dieser Reihenfolge – Betroffenheit klären, patchen, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
FortiCloud-SSO prüfen / einschränken	Patch einspielen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Prüfen, welche Fortinet-Geräte FortiCloud-SSO-Anmeldung aktiviert haben – nur diese sind angreifbar. Inventar über alle betroffenen Produktlinien (FortiOS, FortiProxy, FortiManager, FortiAnalyzer, FortiWeb, FortiNAC-F, FortiSwitchManager) erstellen.

02 SSO-Anmeldung einschränken (vor dem Patch)

FortiCloud-SSO-Login deaktivieren, bis gepatcht ist. FortiOS/FortiProxy:

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

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (z. B. `FortiOS 7.6.6 · 7.4.11 · 7.2.13 · 7.0.19`). Fixversionen je Produkt aus der Tabelle bzw. FG-IR-26-060 übernehmen.

04 Kompromittierung ausschließen

Admin-Konten auf unbekannte Namen prüfen (beobachtet: `audit · backup · itadmin · secadmin · support`), SSO-Logins fremder FortiCloud-Konten, neue/geänderte VPN-Zugänge und Konfigurationsänderungen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Härten & wiederherstellen

Administrativen Zugriff per Local-in-Policy auf definierte Subnetze begrenzen. Bei IoC-Treffern Konfiguration aus einem sauberen Backup wiederherstellen und alle Admin-Zugangsdaten rotieren.

Kompromittierungs-Indikatoren (IoCs)

MISSBRÄUCHLICHE FORTICLOUD-KONTEN

`cloud-noc@mail.io`
`cloud-init@mail.io`

ANGELEGTE ADMIN-KONTEN (PERSISTENZ)

`audit · backup · itadmin`
`secadmin · support`

BEOBACHTETE QUELL-IPS

`104.28.244.115 · 104.28.212.114`
Dritte: `37.1.209.19 · 217.119.139.50`

Zur Einordnung: Die Angreifer wechselten auf Cloudflare-geschützte Adressen – die IPs sind eine flüchtige Momentaufnahme. Verlässlicher ist die Suche nach fremden FortiCloud-SSO-Anmeldungen und unerwartet angelegten Admin-/VPN-Konten in den Geräte-Logs.

Wichtig: Erfolgreiche Anmeldungen erscheinen als reguläre FortiCloud-SSO-Logins – ohne Alarm. Ohne Auswertung der Admin- und SSO-Logs bleibt ein bereits erfolgter Zugriff, angelegte Admin-Konten und neu eingerichtete VPN-Zugänge 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: Fremde FortiCloud-SSO-Anmeldungen und das Anlegen unerwarteter Admin-Konten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden Fortinet-Geräte mit aktivierter FortiCloud-SSO-Anmeldung 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 heute prüfen und bis zum Patch einschränken; Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – angelegte Admin-Konten und VPN-Änderungen dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung administrativer Anmeldungen 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-2026-24858 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-26-060 · Fortinet PSIRT-Blog „Analysis of SSO abuse on FortiOS" · NIST NVD CVE-2026-24858 · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 27.01.2026). 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.