AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-24472

Authentifizierungs-Bypass in Fortinet FortiOS & FortiProxy.

Ein nicht authentifizierter Angreifer aus dem Netz kann über gefälschte CSF-Proxy-Anfragen Super-Admin-Rechte auf einer FortiGate/FortiProxy erlangen – wenn die Security Fabric aktiv ist. Die Schwachstelle ist eine zweite Angriffsvariante zur bereits ausgenutzten CVE-2024-55591 und wird u. a. für die SuperBlack-Ransomware aktiv missbraucht.

> **Geschäftsrisiko:** vollständige Übernahme des Perimeter-Firewalls – mit Potenzial für unbefugten VPN-Zugang, Anlegen von Schatten-Admins, Datenabfluss, Ransomware und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

8,1 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz erreichbar, ohne Rechte, ohne Zutun des Nutzers – erhöhte Angriffskomplexität, da die Seriennummer des Zielgeräts bekannt sein muss; bei Erfolg volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Von NVD mit CVSS 3.1 bewertet; eine CVSS-4.0-Einstufung liegt nicht vor.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Februar 2025	FortiOS 7.0.0–7.0.16 FortiProxy 7.0 & 7.2	Sofort

Das Wichtigste in 60 Sekunden.

8,1 · HOCH
CVSS-Schweregrad

Auth-Bypass
Super-Admin über CSF-Proxy

Aktiv
ausgenutzt · CISA KEV · SuperBlack

Security Fabric
als Voraussetzung nötig

Die Ursache: Verwundbare FortiOS-/FortiProxy-Versionen prüfen bei aktivierter Security Fabric (CSF) nicht ausreichend, ob eine über den Cluster-Synchronisations-Framework weitergeleitete Proxy-Anfrage legitim ist. Kennt der Angreifer die Seriennummer eines Up- oder Downstream-Geräts, kann er über speziell präparierte CSF-Proxy-Anfragen die Authentifizierung umgehen und sich Super-Admin-Rechte verschaffen – ein alternativer Pfad zur selben Wirkung wie die zuvor gemeldete Node.js-WebSocket-Variante (CVE-2024-55591).

ANGRIFFSKETTE

01
Management exponiert – HTTP/HTTPS-Admin-Oberfläche aus dem Netz erreichbar, Security Fabric aktiv

02
Seriennummer beschaffen – Kenntnis der Up-/Downstream-Geräteseriennummer

03
CSF-Proxy missbrauchen – gefälschte Proxy-Anfrage umgeht die Authentifizierung

04
Super-Admin – Schatten-Admins anlegen, SSL-VPN konfigurieren, Zugangsdaten abziehen

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.0	7.0.0 – 7.0.16	7.0.17
FortiOS 7.2 / 7.4 / 7.6	nicht betroffen	—
FortiOS 6.4	nicht betroffen	—
FortiProxy 7.0	7.0.0 – 7.0.19	7.0.20
FortiProxy 7.2	7.2.0 – 7.2.12	7.2.13

Angreifbar nur bei aktivierter **Security Fabric (CSF)** und aus dem Netz erreichbarer Management-Oberfläche. Exakte Build-Ranges gegen das Hersteller-Advisory FG-IR-24-535 des eigenen Zweigs abgleichen; die Fixe decken zugleich CVE-2024-55591 ab.

Regulatorischer Hinweis: Ein bestätigter unbefugter Admin-Zugriff auf die Perimeter-Firewall 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.

ZEITACHSE

14.01.2025
Fortinet veröffentlicht FG-IR-24-535 (CVE-2024-55591)

11.02.2025
CVE-2025-24472 (CSF-Proxy-Variante) ins Advisory aufgenommen

12.03.2025
Forescout: SuperBlack-Ransomware (Mora_001) nutzt die Lücke

18.03.2025
CISA KEV · Frist für Bundesbehörden bis 08.04.2025

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Management absichern / mitigieren	Patch einspielen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Version prüfen (FortiOS 7.0.0–7.0.16, FortiProxy 7.0.0–7.0.19 oder 7.2.0–7.2.12). Ist die Security Fabric (CSF) aktiv? Ist die HTTP/HTTPS-Admin-Oberfläche aus nicht vertrauenswürdigen Netzen erreichbar? Nur diese Kombination ist angreifbar.

02 Sofort mitigieren (vor dem Patch)

Admin-Zugriff auf vertrauenswürdige Quell-IPs beschränken (trusthosts/local-in-policy) und die HTTP/HTTPS-Admin-Oberfläche aus dem Internet nehmen. Wenn nicht benötigt, Security Fabric deaktivieren:

```
config system csf set status disable end
```

03 Patchen

Auf die Fixversion des eigenen Produkts/Zweigs aktualisieren (`FortiOS 7.0.17` · `FortiProxy 7.0.20` · `FortiProxy 7.2.13`). Dieselben Builds schließen auch die verwandte CVE-2024-55591.

04 Kompromittierung ausschließen

Admin-Logs auf verdächtige Anmeldungen und neu angelegte Admin-/Lokal-Konten prüfen und die IoCs unten abgleichen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff. Bei Verdacht: Zugangsdaten rotieren, VPN-/Firewall-Konfiguration auf unbefugte Änderungen prüfen.

05 Perimeter härten

Management-Interfaces grundsätzlich nicht aus dem Internet exponieren, Zugriff über VPN/Jump-Host und Quell-IP-Filter. Herstellerseitige Empfehlungen aus FG-IR-24-535 vollständig umsetzen.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE ADMIN-LOGIN-LOGS

Anmeldungen mit gefälschter `srcip 1.1.1.1`
Konten-Anlage mit `srcip 127.0.0.1`

BEOBACHTETE (GEFÄLSCHTE) QUELL-IPS

`1.1.1.1` · `127.0.0.1` · `2.2.2.2`
`8.8.8.8` · `8.8.4.4` · `13.37.13.37`

AKTIVITÄTSMUSTER

jsconsole-Sitzungen · zufällig benannte Super-Admins
SSL-VPN-Änderungen · Abzug von Zugangsdaten

Zur Einordnung: Die genannten Quell-IPs sind vom Angreifer frei gesetzte Log-Werte (Spoofing), keine echten Herkunftsadressen – auffällig ist gerade ihr Auftauchen in erfolgreichen Admin-Anmeldungen. IoCs sind eine Momentaufnahme der beobachteten Kampagnen und flüchtig; kein Ersatz für die Analyse Ihrer Authentifizierungs-Logs.

Wichtig: Erfolgreiche Angriffe erscheinen als reguläre, erfolgreiche Admin-Anmeldungen und Konten-Anlagen – mit gefälschten Quell-IPs, aber ohne Alarm. Ohne kontinuierliche Auswertung der Admin-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: Admin-Anmeldungen mit gefälschten Quell-IPs und die Anlage unerwarteter Super-Admin-Konten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte FortiGate-/FortiProxy-Management-Oberflächen mit aktiver Security Fabric 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

- Management-Zugriff heute absichern, Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Grundsatz durchsetzen: keine Firewall-Management-Oberfläche im Internet.

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-2025-24472 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-24-535 · NIST NVD CVE-2025-24472 (CVSS 3.1 8,1) · CISA Known Exploited Vulnerabilities Catalog (hinzugefügt 18.03.2025) · Forescout Vedere Labs (SuperBlack / Mora_001). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.