AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-47575

Fehlende Authentifizierung in Fortinet FortiManager („FortiJump").

Der fgfmd-Dienst des FortiManager prüft eingehende Verbindungen nicht ausreichend auf Authentifizierung. Ein nicht authentifizierter Angreifer aus dem Netz kann sich über den FGFM-Port (TCP 541) mit einem gefälschten Gerät verbinden und beliebige Befehle bzw. Code auf der zentralen Management-Plattform ausführen – als Zero-Day seit Juni 2024 aktiv ausgenutzt.

> **Geschäftsrisiko:** vollständige Kompromittierung der zentralen Firewall-Verwaltung – mit Zugriff auf IP-Adressen, Zugangsdaten und Konfigurationen aller verwalteten FortiGate-Geräte, damit Potenzial für flächigen Netzzugriff, Datenabfluss 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 des Nutzers, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Offizieller CVSS-3.1-Basiswert von Fortinet.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
27. Juni 2024	FortiManager 6.2–7.6 + FortiManager Cloud	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Auth fehlt
fgfmd-Dienst · TCP 541

Zero-Day
aktiv ausgenutzt · CISA KEV · PoC öffentlich

> 50 Geräte
kompromittiert (Mandiant, UNC5820)

Die Ursache: Der FortiManager-Dienst **fgfmd** nimmt FGFM-Verbindungen entgegen, ohne die Gegenstelle sicher zu authentifizieren (CWE-306, fehlende Authentifizierung für eine kritische Funktion). Ein Angreifer kann ein beliebiges FortiGate/FortiManager mit einer gefälschten oder von kompromittierten Geräten entwendeten Seriennummer selbst registrieren und anschließend über speziell gestaltete Anfragen Befehle oder Code auf dem FortiManager ausführen.

ANGRIFFSKETTE

01	02	03	04
Port exponiert – der FGFM-Dienst (TCP 541) ist aus dem Netz erreichbar	**Gerät fälschen** – Selbst-Registrierung mit gefälschter oder entwendeter Seriennummer	**Befehle ausführen** – über fgfmd ohne Authentifizierung Code/Befehle ausführen	**Exfiltration** – IPs, Zugangsdaten und Konfigurationen der verwalteten Geräte abziehen

Betroffenheit & Fixversionen

FortiManager-Zweig	Verwundbar bis	Fixversion (Ziel)
7.6	7.6.0	7.6.1
7.4	7.4.0 – 7.4.4	7.4.5
7.2	7.2.0 – 7.2.7	7.2.8
7.0	7.0.0 – 7.0.12	7.0.13
6.4	6.4.0 – 6.4.14	6.4.15
6.2	6.2.0 – 6.2.12	6.2.13
FortiManager Cloud	6.4 · 7.0.1–7.0.12 · 7.2.1–7.2.7 · 7.4.1–7.4.4	Fix-Release je Zweig; 6.4 auf gefixte Version migrieren

Betroffen sind FortiManager und FortiManager Cloud über alle 6.2–7.6-Zweige. Ältere FortiAnalyzer-Modelle im FortiManager-Feature-Modus (7.2.0–7.2.7 / 7.0.1–7.0.12 mit fmg-status enable) sind unter bestimmten Bedingungen ebenfalls betroffen. Exakte Build-Ranges gegen das Hersteller-Advisory FG-IR-24-423 des eigenen Zweigs abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die zentrale Firewall-Verwaltung 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

27.06.2024
Erste beobachtete Ausnutzung (Mandiant)

23.10.2024
Fortinet-Advisory FG-IR-24-423 · CISA KEV · Zero-Day

13.11.2024
CISA-Frist für US-Bundesbehörden (BOD 22-01)

Seither
In Wellen ausgenutzt – UNC5820, > 50

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

FortiManager-Version und -Zweig gegen die Tabelle prüfen. Ist der FGFM-Dienst (TCP 541) aus nicht vertrauenswürdigen Netzen erreichbar? Zentrale Management-Instanzen mit Internet-Exposition sind besonders gefährdet.

02 Sofort mitigieren (vor dem Patch)

Je nach Version einen der von Fortinet benannten Behelfe aktivieren: unbekannte Geräte ablehnen (ab 7.0.12 / 7.2.5 / 7.4.3), Local-in-Policy zur Freigabe nur bekannter FortiGate-IPs auf Port 541, oder exklusive CA-Zertifikate erzwingen (ab 7.2.2 / 7.4.0 / 7.6.0).

```
config system global set fgfm-deny-unknown enable end
```

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`7.6.1` · `7.4.5` · `7.2.8` · `7.0.13` · `6.4.15` · `6.2.13`). FortiManager-Cloud-Umgebungen mit Fortinet abstimmen bzw. 6.4 auf eine gefixte Version migrieren.

04 Kompromittierung ausschließen

Geräte-Logs auf unregistrierte Geräte-Hinzufügungen und Änderungen mit veränderten Seriennummern durchsuchen, die IoCs unten abgleichen und die verwalteten FortiGate-Zugangsdaten als potenziell offengelegt behandeln. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Nach Kompromittierung: Zugangsdaten rotieren

Bei Verdacht auf Ausnutzung alle auf dem FortiManager gespeicherten Zugangsdaten und die der verwalteten Geräte rotieren, Konfigurationen auf unautorisierte Änderungen prüfen und die herstellerseitige Recovery-Anleitung von Fortinet befolgen.

Kompromittierungs-Indikatoren (IoCs)

ANGREIFER-QUELL-IPS

`45.32.41.202` · `104.238.141.143`
`158.247.199.37` · `45.32.63.2` · `80.66.196.199`
`198.199.122.22` · `142.93.177.233`
`195.85.114.78` · `172.232.167.68`

VERDÄCHTIGE SERIENNUMMERN

`FMG-VMTM23017412`
`FMG-VMTM19008093`
`FGVMEVWG8YMT3R63`

DATEIEN & LOG-MARKER

`/tmp/.tm` · `/var/tmp/.tm`
Log-Einträge: unregistrierte Geräte-Adds und Geräte-Änderungen mit veränderter Seriennummer

Zur Einordnung: IPs und Seriennummern sind eine Momentaufnahme der beobachteten Kampagne und flüchtig – kein Ersatz für die Analyse Ihrer FortiManager-Logs. Auffällig sind vor allem unregistrierte Geräte-Hinzufügungen und Seriennummern-Manipulationen im dvm-Log.

Wichtig: Erfolgreiche Ausnutzung erscheint als reguläre Geräte-Registrierung im Management-Log – ohne Alarm. Ohne kontinuierliche Auswertung der FortiManager-Logs bleibt ein bereits erfolgter Zugriff auf die zentrale Firewall-Verwaltung 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: Unregistrierte Geräte-Hinzufügungen und Seriennummern-Manipulationen im FortiManager-Log fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte FortiManager-Instanzen mit erreichbarem FGFM-Port (TCP 541) 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 FortiManager-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

- Zugriff auf den FGFM-Port heute einschränken, Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung; bei Verdacht Zugangsdaten der verwalteten Geräte rotieren.
- Über eine dauerhafte Überwachung von Management-Plattformen und Perimeter 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-2024-47575 und dem FortiManager-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-24-423 (CVE-2024-47575) · NIST NVD CVE-2024-47575 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 23.10.2024) · Mandiant / Google Threat Intelligence „Investigating FortiManager Zero-Day Exploitation (CVE-2024-47575)". 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.