AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-23113

Format-String-RCE im Fortinet fgfmd-Dienst.

Ein nicht authentifizierter Angreifer aus dem Netz kann über den FGFM-Dienst (fgfmd-Daemon) speziell gestaltete Anfragen senden und darüber beliebigen Code oder Befehle ausführen – ohne gültige Anmeldedaten. Ursache ist eine Format-String-Schwachstelle (CWE-134). Praktisch angreifbar ist jedes Gerät mit erreichbarem FGFM-Interface; die Ausnutzung läuft laut CISA/Fortinet seit Oktober 2024.

> **Geschäftsrisiko:** vollständige Kompromittierung der Firewall bzw. des Sicherheits-Gateways – mit Potenzial für Umgehung der Perimeter-Kontrollen, Zugriff auf das interne Netz, Persistenz 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 – volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD-Basiswert 9,8 (CVSS 3.1, von Fortinet vergeben); Fortinet weist im Advisory zusätzlich die Exploit-Reife „hoch" (E:H, RC:C) aus. Eine CVSS-4.0-Bewertung liegt beim NVD nicht vor.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Oktober 2024	FortiOS · FortiProxy · FortiPAM · FortiSwitchManager (FGFM)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Pre-Auth-RCE
Format String im fgfmd-Daemon

Aktiv
ausgenutzt · CISA KEV (seit 09.10.2024)

CWE-134
externbeeinflusster Format String

Die Ursache: Der `fgfmd`-Daemon wickelt das FGFM-Protokoll für die Kommunikation zwischen FortiGate/FortiOS und FortiManager ab. Beim Verarbeiten eingehender FGFM-Anfragen fließt ein extern beeinflusster Wert ungeprüft als **Format-String** in eine Verarbeitungsfunktion (CWE-134). Ein entfernter, nicht authentifizierter Angreifer kann darüber mit speziell gestalteten Paketen den Speicher manipulieren und bis zur **Ausführung beliebiger Befehle** eskalieren.

ANGRIFFSKETTE

01
FGFM exponiert – der FGFM-Dienst (Standard-Port TCP 541) ist über eine Interface-`allowaccess`-Freigabe aus dem Netz erreichbar

02
Verbindung aufbauen – der Angreifer spricht den fgfmd-Daemon an, der eingehende FGFM-Anfragen entgegennimmt

03
Format-String einschleusen – ein speziell gestalteter, extern beeinflusster Wert wird als Format-String verarbeitet (CWE-134)

04
Codeausführung – daraus folgt die Ausführung beliebiger Befehle / beliebigen Codes auf dem Gerät

Betroffenheit & Fixversionen

Produkt · Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.4	`7.4.0 – 7.4.2`	`7.4.3`
FortiOS 7.2	`7.2.0 – 7.2.6`	`7.2.7`
FortiOS 7.0	`7.0.0 – 7.0.13`	`7.0.14`
FortiProxy 7.4 / 7.2 / 7.0	`7.4.0–7.4.2 · 7.2.0–7.2.8 · 7.0.0–7.0.15`	`7.4.3 · 7.2.9 · 7.0.16`
FortiPAM 1.0 – 1.2	alle Versionen (1.0 / 1.1 / 1.2)	auf gepatchten Release migrieren
FortiSwitchManager 7.2 / 7.0	`7.2.0–7.2.3 · 7.0.0–7.0.3`	`7.2.4 · 7.0.4`

Praktisch angreifbar sind Geräte mit erreichbarem FGFM-Interface. Der CISA-KEV-Eintrag nennt als betroffen zusätzlich **FortiWeb**; die exakten Versionsbereiche dafür im Hersteller-Advisory prüfen. Alle Build-Ranges und Fixversionen gegen das Advisory FG-IR-24-029 des eigenen Zweigs abgleichen.

Regulatorischer Hinweis: Eine bestätigte Codeausführung bzw. ein unbefugter Zugriff auf Firewall/Gateway 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

15.02.2024 | 09.10.2024 | 11.10.2024 | 30.10.2024 | Stand heute

Ihr Maßnahmenplan.

In dieser Reihenfolge – FGFM abschotten vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
FGFM-Zugriff einschränken	Patch einspielen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Produkt und Version prüfen (FortiOS, FortiProxy, FortiPAM, FortiSwitchManager – gegen die Tabelle abgleichen). Ist der FGFM-Dienst über eine Interface-`allowaccess`-Freigabe aus dem Internet oder aus nicht vertrauenswürdigen Netzen erreichbar? Nur exponierte FGFM-Interfaces sind praktisch angreifbar.

02 Sofort mitigieren (vor dem Patch)

Herstellerbehelf: `fgfm` aus `allowaccess` der exponierten Interfaces entfernen (Hinweis: dies unterbindet die FortiManager-Erkennung). Alternativ per Local-in-Policy auf vertrauenswürdige Hosts beschränken:

```
config system interface edit <port> set allowaccess ping https ssh next end
```

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (u. a. FortiOS `7.4.3` · `7.2.7` · `7.0.14`, FortiProxy `7.4.3` · `7.2.9` · `7.0.16`, FortiSwitchManager `7.2.4` · `7.0.4`). Für FortiPAM 1.0–1.2 auf einen gepatchten Release migrieren. Fortinet hat für die betroffenen Zweige feste Builds veröffentlicht.

04 Kompromittierung ausschließen

Logs auf unerwartete FGFM-Verbindungen aus fremden Quellen sowie auf Abstürze/Neustarts des `fgfmd`-Prozesses prüfen und die Konfiguration auf unautorisierte Änderungen kontrollieren. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Perimeter härten

Grundsatz durchsetzen: Management- und FGFM-Dienste nie direkt exponieren, sondern auf vertrauenswürdige Netze / VPN beschränken. Herstellerseitige IPS-Signaturen für diese Schwachstelle einspielen, sofern verfügbar.

Kompromittierungs-Indikatoren (IoCs)

EXPONIERTER DIENST

FGFM auf TCP `541` · Interfaces mit `fgfm` in `allowaccess`

AUFFÄLLIGE AKTIVITÄT

FGFM-Verbindungsversuche aus unerwarteten Quell-IPs · Abstürze / Neustarts des `fgfmd`-Prozesses in den Logs

KONFIGURATIONS-DRIFT

unautorisierte Änderungen an Admin-Konten, Policies oder Systemkonfiguration nach FGFM-Zugriff

Zur Einordnung: Für diese Schwachstelle liegen keine belastbaren, herstellerbestätigten netzwerkbasierten IoCs vor; die genannten Marker sind allgemeine Prüfhinweise und kein Ersatz für die Analyse Ihrer Zugriffs-, System- und Krash-Logs. Ein reiner Format-String-Angriff kann sehr wenige Spuren hinterlassen.

Wichtig: Eine erfolgreiche Ausnutzung ermöglicht Codeausführung ohne Anmeldung. Ein reiner Patch entfernt bereits etablierte Persistenz, geänderte Konfiguration oder Konten nicht – ohne Prüfung des Systems bleibt eine erfolgte Kompromittierung 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: FGFM-Verbindungen aus fremden Quellen und Abstürze des fgfmd-Prozesses fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte Fortinet-Geräte mit erreichbarem FGFM-Dienst 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 · fgfmd-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

- FGFM-Zugriff heute einschränken, Patch kurzfristig (CISA-Frist war 30.10.2024) einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Grundsatz durchsetzen: Management- und FGFM-Dienste nie direkt exponieren.

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-2024-23113 und dem FortiOS · fgfmd-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-24-029 (CVE-2024-23113) · NVD (nvd.nist.gov, CVSS 3.1 Basiswert 9,8, CWE-134) · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 09.10.2024, Frist 30.10.2024, Ransomware-Nutzung: unbekannt). 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.