THREAT INTELLIGENCE BRIEFING

CVE-2026-126261

Codeausführung über den FGFM-Dienst von FortiManager.

Der FGFM-Dienst von FortiManager, über den sich FortiGate-Firewalls an der zentralen Verwaltung anmelden, vergibt Rechte, bevor das Registrierungspasswort geprüft ist. Ein Angreifer ohne Anmeldung, der den FGFM-Port erreicht, kann dadurch Code oder Befehle ausführen. Fortinet hat die Lücke am 10.11.2026 mit 8.0.1, 7.6.8, 7.4.6 und 7.2.9 geschlossen; eine Ausnutzung ist bislang nicht bekannt.

Geschäftsrisiko: Übernahme der zentralen Firewall-Verwaltung – mit Zugriff auf Konfigurationen und Zugangsdaten aller verwalteten FortiGates, Einstieg ins Firmennetz und einem 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 Anmeldung, ohne Mitwirkung eines Nutzers, mit voller Wirkung auf das System. Basiswert laut NVD (Vektor von Fortinet als CNA); das Fortinet-Advisory nennt 9,0.

AUSNUTZUNG
Nicht bekannt (Stand 11.11.2026)

BETROFFEN
FortiManager 8.0.0, 7.6.0–7.6.7
7.4.0–7.4.5, 7.2.0–7.2.8

HANDLUNGSBEDARF
Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
FGFM-Dienst · CWE-285

Nicht bekannt
Ausnutzung · nicht in CISA KEV · kein PoC öffentlich

8.0.1 · 7.6.8 · 7.4.6 · 7.2.9
Fixversionen seit 10.11.2026

Die Ursache: Über das **FGFM-Protokoll** (FortiGate-to-FortiManager) melden sich verwaltete FortiGates bei FortiManager an. Laut Fortinet erhält eine Gegenstelle dabei erweiterte Rechte, **bevor das Registrierungspasswort geprüft ist** (**CWE-285, Improper Authorization**). Ein nicht authentifizierter Angreifer, der den FGFM-Port erreicht, kann so mit präparierten FGFM-Paketen Code oder Befehle ausführen. Fortinet hat die Lücke intern gefunden und nennt keine weiteren technischen Details.

ANGRIFFSKETTE

01 **Port erreichbar** – FGFM-Dienst von FortiManager ist aus dem Netz ansprechbar

02 **Präparierte Pakete** – Angreifer sendet FGFM-Nachrichten ohne gültige Registrierung

03 **Rechte zu früh** – Berechtigung wird vor der Passwortprüfung erteilt

04 **Codeausführung** – Befehle auf FortiManager, Zugriff auf verwaltete Geräte

Betroffenheit & Fixversionen

Produkt · Zweig	Verwundbar bis	Fixversion (Ziel)
FortiManager 8.0	8.0.0	8.0.1
FortiManager 7.6	7.6.0 bis 7.6.7	7.6.8
FortiManager 7.4	7.4.0 bis 7.4.5	7.4.6
FortiManager 7.2	7.2.0 bis 7.2.8	7.2.9

Angaben laut Fortinet-Advisory FG-IR-26-275. Fortinet nennt **keinen Workaround** und keinen virtuellen Patch. Ältere Zweige führt das Advisory nicht auf. Voraussetzung für einen Angriff ist, dass der FGFM-Port von FortiManager erreichbar ist.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die 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

10.11.2026
CVE-Nummer reserviert

10.11.2026
FG-IR-26-275 · Fix 8.0.1 / 7.6.8 / 7.4.6 / 7.2.9

10.11.2026
Fortinet: keine Ausnutzung bekannt

Stand heute
Nicht in CISA KEV · kein PoC

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
FGFM-Zugriff begrenzen	Update einspielen	Logs prüfen

01 Betroffenheit feststellen

Version aller FortiManager-Instanzen prüfen: `8.0.0`, `7.6.0`–`7.6.7`, `7.4.0`–`7.4.5` und `7.2.0`–`7.2.8` sind betroffen. Klären, von wo der FGFM-Port erreichbar ist.

02 Patchen

Auf `8.0.1`, `7.6.8`, `7.4.6` bzw. `7.2.9` oder neuer aktualisieren. Vorher ein Konfigurations-Backup sichern.

03 Risiko bis zum Update senken

Fortinet nennt keinen Workaround. Den FGFM-Port per Firewall-Regel nur für die bekannten Adressen der verwalteten FortiGates öffnen, nie für das gesamte Internet.

04 Kompromittierung ausschließen

Event-Logs auf unbekannte Geräte-Registrierungen und unerwartete Konfigurationsänderungen prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Fortinet nennt keine, Ausnutzung nicht bekannt

AUSWERTUNGSQUELLEN

FortiManager-Event-Logs
Firewall-Logs zum FGFM-Port

AUFFÄLLIGE MUSTER

FGFM-Verbindungen von unbekannten Adressen
unerwartete Geräte oder Konfigurationsänderungen

Zur Einordnung: Es liegen keine CVE-spezifischen Indikatoren vor. Die genannten Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

Wichtig: FortiManager hält Konfigurationen und Zugangsdaten aller verwalteten Firewalls. Wer die Verwaltung übernimmt, steuert damit das gesamte Firewall-Netz.

Bildmotive: KI-generierte Symbolbilder

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: Eine FGFM-Verbindung von einer unbekannten Adresse 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 FortiManager 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

- Update aller FortiManager-Instanzen auf die Fixversionen anordnen.
- Bestätigen lassen, dass die Verwaltung nicht offen im Internet steht.
- Über eine dauerhafte Überwachung der Firewall-Verwaltung 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-2026-126261 und dem FortiManager-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Fortinet PSIRT FG-IR-26-275 (10.11.2026, Fixversionen, CVSS 9,0) · NVD (CVSS 3.1 Basiswert 9,8) · CISA KEV (Stand 11.11.2026: nicht gelistet). Stand 11.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.