THREAT INTELLIGENCE BRIEFING

CVE-2026-126262

Codeausführung per SQL-Injection über den OFTP-Dienst.

Über den OFTP-Dienst senden FortiGate-Firewalls ihre Logs an FortiAnalyzer und FortiManager. Eine SQL-Injection in diesem Dienst erlaubt einem Angreifer ohne Anmeldung, der den OFTP-Port erreicht, mit präparierten OFTP-Paketen Code oder Befehle auszuführen. Fortinet hat die Lücke am 10.11.2026 in allen vier unterstützten Zweigen beider Produkte geschlossen; eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** Übernahme der zentralen Log- und Firewall-Verwaltung – mit Zugriff auf Sicherheitsprotokolle, Konfigurationen und Zugangsdaten verwalteter FortiGates, der Möglichkeit, Spuren zu verwischen, 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 9,3.

AUSNUTZUNG
Nicht bekannt (Stand 11.11.2026)

BETROFFEN
FortiAnalyzer 8.0.0–8.0.1, 7.6.0–7.6.7, 7.4.0–7.4.11, 7.2.0–7.2.12
FortiManager 8.0.0, 7.6.0–7.6.7, 7.4.0–7.4.11, 7.2.0–7.2.12

HANDLUNGSBEDARF
Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
OFTP-Dienst · CWE-89

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

8.0.2/8.0.1 · 7.6.8 · 7.4.12 · 7.2.13
Fixversionen seit 10.11.2026

Die Ursache: Über das **OFTP-Protokoll** übertragen FortiGates Logs und Statusdaten an FortiAnalyzer bzw. an FortiManager. Laut Fortinet werden Inhalte empfangener OFTP-Pakete nicht ausreichend bereinigt, bevor sie in eine Datenbankabfrage einfließen (**CWE-89, SQL Injection**). Ein **nicht authentifizierter Angreifer**, der den OFTP-Port erreicht, kann so mit präparierten OFTP-Paketen Code oder Befehle auf dem System ausführen. Fortinet hat die Lücke intern gefunden und nennt keine weiteren technischen Details.

ANGRIFFSKETTE

01	02	03	04
Port erreichbar – OFTP-Dienst von FortiAnalyzer/FortiManager ist aus dem Netz ansprechbar	**Präparierte Pakete** – Angreifer sendet OFTP-Nachrichten ohne Anmeldung	**SQL-Injection** – eingeschleuste Befehle gelangen ungefiltert in die Datenbankabfrage	**Codeausführung** – Befehle auf dem System, Zugriff auf Logs und verwaltete Geräte

Betroffenheit & Fixversionen

Produkt · Zweig	Verwundbar bis	Fixversion (Ziel)
FortiAnalyzer 8.0	8.0.0 bis 8.0.1	8.0.2
FortiAnalyzer 7.6	7.6.0 bis 7.6.7	7.6.8
FortiAnalyzer 7.4	7.4.0 bis 7.4.11	7.4.12
FortiAnalyzer 7.2	7.2.0 bis 7.2.12	7.2.13
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 7.4.11	7.4.12
FortiManager 7.2	7.2.0 bis 7.2.12	7.2.13

Angaben laut Fortinet-Advisory FG-IR-26-276. Fortinet nennt **keinen Workaround** und keinen virtuellen Patch. Ältere Zweige führt das Advisory nicht auf. Voraussetzung für einen Angriff ist, dass der OFTP-Port von FortiAnalyzer bzw. FortiManager erreichbar ist.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die Log- oder 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.

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
OFTP-Zugriff begrenzen	Update einspielen	Logs prüfen

01 Betroffenheit feststellen

Version aller FortiAnalyzer- und FortiManager-Instanzen prüfen. FortiAnalyzer: `8.0.0`–`8.0.1`, `7.6.0`–`7.6.7`, `7.4.0`–`7.4.11`, `7.2.0`–`7.2.12`. FortiManager: `8.0.0`, `7.6.0`–`7.6.7`, `7.4.0`–`7.4.11`, `7.2.0`–`7.2.12`. Klären, von wo der OFTP-Port erreichbar ist.

02 Patchen

FortiAnalyzer auf `8.0.2`, `7.6.8`, `7.4.12` bzw. `7.2.13`, FortiManager auf `8.0.1`, `7.6.8`, `7.4.12` bzw. `7.2.13` oder neuer aktualisieren. Vorher ein Konfigurations-Backup sichern.

03 Risiko bis zum Update senken

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

04 Kompromittierung ausschließen

Event-Logs auf unbekannte Geräte, unerwartete Konfigurationsänderungen und Lücken in der Log-Historie prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Fortinet nennt keine, Ausnutzung nicht bekannt

AUSWERTUNGSQUELLEN

FortiAnalyzer-/FortiManager-Event-Logs
Firewall-Logs zum OFTP-Port

AUFFÄLLIGE MUSTER

OFTP-Verbindungen von unbekannten Adressen
unerwartete Geräte, Konfigurationsänderungen oder Log-Lücken

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

Wichtig: FortiAnalyzer und FortiManager bündeln die Sicherheitsprotokolle und Konfigurationen der angebundenen Firewalls. Wer sie übernimmt, sieht das Netz – und kann eigene Spuren verwischen.

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 OFTP-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 FortiAnalyzer und 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 FortiAnalyzer-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 FortiAnalyzer- und FortiManager-Instanzen auf die Fixversionen anordnen.
- Bestätigen lassen, dass Log- und Firewall-Verwaltung nicht offen im Internet stehen.
- 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-2026-126262 und dem FortiAnalyzer-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Fortinet PSIRT FG-IR-26-276 (10.11.2026, Fixversionen, CVSS 9,3) · NVD (11.11.2026, 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.