THREAT INTELLIGENCE BRIEFING

CVE-2026-126170

Codeausführung über die JSON-API von FortiAnalyzer und FortiManager.

Die JSON-API (JSON-RPC) der Weboberfläche von FortiAnalyzer und FortiManager kodiert Ausgaben nicht korrekt. Ein Angreifer ohne Anmeldung kann dadurch mit einer präparierten HTTP-Anfrage Code oder Befehle ausführen – sofern die standardmäßig deaktivierte JSON-API in einem Admin-Profil freigeschaltet ist. Fortinet hat am 10.11.2026 die Fixversion 7.6.8 veröffentlicht; für die 8.0-Zweige und FortiAnalyzer-BigData sind 8.0.3 bzw. 7.6.3 angekündigt, bis dahin gilt der Workaround. Eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** Übernahme der zentralen Firewall-Verwaltung bzw. der Log-Plattform – mit Zugriff auf Konfigurationen, Zugangsdaten und Protokolle, 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 ebenfalls 9,8 (temporär 8,9).

AUSNUTZUNG	BETROFFEN	HANDLUNGSBEDARF
Nicht bekannt (Stand 11.11.2026)	FortiAnalyzer / FortiManager 8.0.0–8.0.2, 7.6.0–7.6.7 Cloud 8.0.1–8.0.2, 7.6.0–7.6.7 · BigData 7.6.0–7.6.2	Dringend – JSON-API prüfen, patchen oder abschalten

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
JSON-API der Weboberfläche · CWE-116

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

7.6.8 · 8.0.3 angekündigt
Fixversionen · Workaround verfügbar

Die Ursache: Fortinet beschreibt eine **JSON-Injection in der JRPC-API** der Weboberfläche: Ausgaben werden nicht korrekt kodiert bzw. maskiert (**CWE-116, Improper Encoding or Escaping of Output**). Ein nicht authentifizierter Angreifer kann so über eine **präparierte HTTP-Anfrage** Code oder Befehle ausführen. Betroffen sind laut Fortinet nur Systeme, auf denen die **JSON-API in einem Admin-Profil aktiviert** ist – standardmäßig ist sie deaktiviert. Fortinet hat die Lücke intern gefunden und nennt keine weiteren technischen Details.

ANGRIFFSKETTE

01	02	03	04
API erreichbar – Weboberfläche mit aktivierter JSON-API ist aus dem Netz ansprechbar	**Präparierte Anfrage** – Angreifer sendet eine HTTP-Anfrage ohne Anmeldung	**JSON-Injection** – fehlerhafte Kodierung lässt eingeschleuste Daten wirken	**Codeausführung** – Befehle auf FortiAnalyzer bzw. FortiManager

Betroffenheit & Fixversionen

Produkt · Zweig	Verwundbar bis	Fixversion (Ziel)
FortiAnalyzer / FortiManager 8.0	`8.0.0 bis 8.0.2`	8.0.3 (angekündigt) · bis dahin Workaround
FortiAnalyzer / FortiManager 7.6	`7.6.0 bis 7.6.7`	`7.6.8`
FortiAnalyzer Cloud / FortiManager Cloud 8.0	`8.0.1 bis 8.0.2`	8.0.3 (angekündigt) · bis dahin Workaround
FortiAnalyzer Cloud / FortiManager Cloud 7.6	`7.6.0 bis 7.6.7`	`7.6.8`
FortiAnalyzer-BigData 7.6	`7.6.0 bis 7.6.2`	7.6.3 (angekündigt) · bis dahin Workaround

Angaben laut Fortinet-Advisory FG-IR-26-219. Die Zweige 7.4 und 7.2 aller genannten Produkte sind **nicht betroffen**. Fortinet nennt einen **Workaround**: die JSON-API im Admin-Profil abschalten (`set rpc-permit none`). Zusätzlich führt das Advisory FortiSASE-Sovereign 25, 25.3 und 25.4 (alle Versionen, Migration auf eine behobene Version) auf; 26.2 ist laut Fortinet bereits behoben.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die Firewall-Verwaltung oder die Log-Plattform kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung übernehmen wir nicht, wir unterstützen bei Bewertung und Dokumentation.

Seite 3: Ihr Maßnahmenplan →

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
JSON-API prüfen und abschalten	Update einspielen	Logs prüfen

01 Betroffenheit feststellen

Version aller FortiAnalyzer-, FortiManager- und BigData-Instanzen prüfen: `8.0.0`–`8.0.2` und `7.6.0`–`7.6.7` (BigData `7.6.0`–`7.6.2`) sind betroffen. Prüfen, ob in einem Admin-Profil die JSON-API aktiviert ist, und klären, von wo die Weboberfläche erreichbar ist.

02 Patchen

Im Zweig 7.6 auf `7.6.8` oder neuer aktualisieren. Für 8.0 (`8.0.3`) und BigData (`7.6.3`) sind die Fixversionen angekündigt – nach Erscheinen zügig einspielen. Vorher ein Konfigurations-Backup sichern.

03 Workaround bis zum Update

Laut Fortinet die JSON-API in jedem Admin-Profil abschalten: `config system admin profile` → `edit <Profil>` → `set rpc-permit none` → `end`. Vorher klären, welche Automatisierungen die API nutzen. Die Weboberfläche zusätzlich nur aus dem Verwaltungsnetz erreichbar machen.

04 Kompromittierung ausschließen

Event-Logs auf unbekannte API-Zugriffe, neue Administratoren 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

FortiAnalyzer-/FortiManager-Event-Logs
Web- und Firewall-Logs zur Weboberfläche

AUFFÄLLIGE MUSTER

JSON-RPC-Anfragen von unbekannten Adressen
neue Admins oder unerwartete 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, FortiAnalyzer die Protokolle des gesamten Netzes. Wer diese Systeme übernimmt, steuert das Firewall-Netz und kann 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 JSON-RPC-Anfrage 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 / 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 / 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 auf 7.6.8 bzw. die angekündigten Fixversionen anordnen – bis dahin JSON-API abschalten.
- Bestätigen lassen, dass Verwaltung und Log-Plattform 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-2026-126170 und dem FortiAnalyzer / 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-26-219 (10.11.2026, Fixversionen, Workaround, CVSS 9,8) · 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.