AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-21643

Unauthentifizierte SQL-Injektion in Fortinet FortiClient EMS.

Ein nicht authentifizierter Angreifer aus dem Internet kann über eine speziell präparierte HTTP-Anfrage SQL-Befehle in die Administrationsschnittstelle von FortiClient EMS einschleusen und unbefugt Code oder Kommandos ausführen – ohne Anmeldung, mit voller Wirkung auf das System. Die Lücke wird seit März 2026 aktiv ausgenutzt und steht im CISA-KEV-Katalog.

> **Geschäftsrisiko:** vollständige Kompromittierung des zentralen Endpoint-Management-Servers – mit Potenzial für Datenabfluss, Übernahme der verwalteten Endpunkte, Betriebsunterbrechung 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, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Fortinet weist im eigenen Advisory 9,1 aus – derselbe Basiswert, jedoch um Ausnutzungs- und Remediation-Metriken (E:F/RL:O/RC:C) ergänzt.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
März 2026	FortiClient EMS 7.4.4 (nur 7.4-Zweig)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Basiswert (NVD)

SQL-Injektion
Unauth. Code-/Kommando-Ausführung

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

7.2 & 8.0
Zweige nicht betroffen

Die Ursache: Die administrative Schnittstelle von FortiClient EMS übergibt einen aus der HTTP-Anfrage stammenden Wert – den zur Mandanten-Zuordnung genutzten Header – ungefiltert an eine Datenbankabfrage, und zwar **vor jeder Anmeldeprüfung**. Ein Angreifer kann dadurch eigene SQL-Anweisungen in die Abfrage einschleusen (CWE-89) und über die Datenbank unbefugt Code oder Betriebssystem-Kommandos ausführen – ohne gültiges Konto.

ANGRIFFSKETTE

01 **EMS exponiert** – die administrative Schnittstelle ist aus dem Internet erreichbar

02 **Header manipulieren** – SQL-Payload in den Mandanten-Header der HTTP-Anfrage einbetten

03 **Injektion vor Login** – die ungeprüfte Abfrage wird ohne Authentifizierung ausgeführt

04 **Ausführung** – unbefugte Code-/Kommando-Ausführung bis zur Server-Übernahme

Betroffenheit & Fixversionen

EMS-Zweig	Verwundbar bis	Fixversion (Ziel)
7.4	nur 7.4.4	7.4.5
7.2	nicht betroffen	—
8.0	nicht betroffen	—

Betroffen ist ausschließlich FortiClient EMS **7.4.4**; die Zweige 7.2 und 8.0 sind laut Fortinet nicht angreifbar. Exponiert ist vor allem, wer die EMS-Administrationsschnittstelle aus dem Internet erreichbar hält. Die exakte Version gegen das Hersteller-Advisory FG-IR-25-1142 abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf den zentralen Management-Server 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

06.02.2026
Fortinet veröffentlicht Advisory FG-IR-25-1142

März 2026
Aktive Ausnutzung in der Wildnis beobachtet

13.04.2026
CISA KEV · PoC öffentlich verfügbar

Seither
Fortlaufende Ausnutzung exponierter EMS-Instanzen

Ihr Maßnahmenplan.

In dieser Reihenfolge – Perimeter absichern vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Adminschnittstelle vom Internet trennen	Patch einspielen	Threat Hunting / Log-Analyse

01 Betroffenheit feststellen

Installierte FortiClient-EMS-Version prüfen: Nur `7.4.4` ist angreifbar. Zweige 7.2 und 8.0 sind nicht betroffen. Zusätzlich klären, ob die EMS-Administrationsschnittstelle aus dem Internet erreichbar ist – das erhöht die Dringlichkeit erheblich.

02 Sofort absichern (vor dem Patch)

Fortinet nennt keinen Workaround. Bis zum Patch die administrative Schnittstelle vom Internet trennen bzw. den Zugriff strikt auf vertrauenswürdige Quell-Netze/VPN einschränken und vorgelagerte Web-Filter/WAF-Regeln gegen SQL-Injektionsmuster aktivieren.

03 Patchen

Auf `FortiClient EMS 7.4.5` oder höher aktualisieren. Das ist die vom Hersteller bestätigte Fixversion für den 7.4-Zweig.

04 Kompromittierung ausschließen

Zugriffs- und Datenbank-Logs der EMS auf ungewöhnliche HTTP-Anfragen an die Adminschnittstelle, SQL-Fehler und neu angelegte oder veränderte Administratorkonten durchsuchen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Verwaltete Endpunkte bewerten

Da EMS die FortiClient-Endpunkte zentral steuert, bei Verdacht auf Kompromittierung Richtlinien-, Zertifikats- und Deployment-Integrität prüfen und ggf. Anmeldedaten/Token rotieren.

Kompromittierungs-Indikatoren (IoCs)

ANGRIFFSZIEL	INJEKTIONS-MARKER	FOLGE-SPUREN
HTTP(S)-Anfragen an die `EMS-Administrationsschnittstelle` aus unerwarteten Quellen	SQL-Syntax im `Mandanten-/Tenant-Header` der Anfrage	neu angelegte / veränderte `Admin-Konten`
	anomale DB-Fehler in den EMS-Logs	unerwartete Prozess-/Kommandoausführung auf dem EMS-Host

Zur Einordnung: Fortinet und CISA haben zum Stand dieses Advisories keine belastbaren netzbasierten IoCs (Quell-IPs, Hashes) in den Primärquellen veröffentlicht. Die genannten Marker sind Erkennungshinweise, kein abschließender IoC-Satz – maßgeblich ist die Analyse Ihrer EMS-Zugriffs- und Datenbank-Logs.

Wichtig: Die Injektion greift vor der Anmeldung und kann in regulären HTTP-Logs unauffällig wirken. Ohne gezielte Auswertung der EMS-Zugriffs- und Datenbank-Logs bleibt ein bereits erfolgter Zugriff leicht 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: Anomale Anfragen an die EMS-Adminschnittstelle und neu angelegte Administratorkonten 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, ungepatchte FortiClient-EMS-7.4.4-Instanzen 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 FortiClient EMS-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

- Adminschnittstelle heute vom Internet trennen, Patch auf 7.4.5 innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung des Perimeters und der Management-Server 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-2026-21643 und dem FortiClient EMS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-25-1142 (CVE-2026-21643) · NVD CVE-2026-21643 · CISA Known Exploited Vulnerabilities Catalog. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion (7.4.5) und Betroffenheit gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.