AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2023-48788

Unauthentifizierte SQL-Injection in Fortinet FortiClientEMS.

Ein nicht authentifizierter Angreifer aus dem Netz kann über eine SQL-Injection eigene Datenbankbefehle in FortiClientEMS einschleusen. Weil der Data-Access-Server die manipulierten Anfragen an einen Microsoft-SQL-Server weiterreicht, lässt sich der Angriff bis zur Ausführung beliebiger Systembefehle ausweiten – FortiClientEMS verwaltet zentral die Endpunkt-Sicherheit ganzer Unternehmen. Die Schwachstelle wird seit März 2024 aktiv ausgenutzt und steht im CISA-KEV-Katalog.

> **Geschäftsrisiko:** Vollständige Übernahme des zentralen Endpunkt-Management-Servers und der dahinterliegenden Datenbank – mit Potenzial für Ausbreitung auf verwaltete Endpunkte, Datenabfluss, 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 – vollständige Kontrolle über Vertraulichkeit, Integrität und Verfügbarkeit; über die eingebettete Datenbank bis hin zur Ausführung eigener Befehle auf dem Server. Fortinet selbst bewertet die Lücke mit 9,3.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
März 2024	FortiClientEMS 7.2.0–7.2.2 FortiClientEMS 7.0.1–7.0.10	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1)

Unauth SQLi → RCE
ohne Anmeldung bis zur Befehlsausführung

Aktiv
ausgenutzt · CISA KEV (seit 25.03.2024)

CWE-89
SQL-Injection

Die Ursache: Der Dienst `FmcDaemon` von FortiClientEMS nimmt auf TCP-Port `8013` Verbindungen entgegen und übergibt einen vom Client kontrollierten Parameter (FCTUID) ohne ausreichende Prüfung an den Data-Access-Server (`FCTDas`). Dieser setzt die Anfrage in eine SQL-Abfrage gegen einen Microsoft-SQL-Server um. Ein nicht authentifizierter Angreifer kann so eigene SQL-Befehle einschleusen und – durch Aktivieren von `xp_cmdshell` – Systembefehle mit den Rechten des Datenbankdienstes ausführen.

ANGRIFFSKETTE

01	02	03	04
FmcDaemon exponiert – TCP-Port `8013` ist über das Netz erreichbar	**SQL einschleusen** – manipulierter, unauthentifizierter FCTUID in einer präparierten Anfrage	**Datenbank ausführen** – der Data-Access-Server reicht die Injection an den Microsoft-SQL-Server weiter	**Ausweitung** – über `xp_cmdshell` beliebige Systembefehle und Übernahme des Servers

Betroffenheit & Fixversionen

FortiClientEMS-Version	Verwundbar bis	Fixversion (Ziel)
FortiClientEMS 7.2	`7.2.0 - 7.2.2`	`7.2.3`
FortiClientEMS 7.0	`7.0.1 - 7.0.10`	`7.0.11`
FortiClientEMS 6.4	nicht betroffen	—

Betroffen sind FortiClientEMS `7.2.0` bis `7.2.2` sowie `7.0.1` bis `7.0.10`. Fortinet stellt die Fixes in `7.2.3` und `7.0.11` bereit; Version 6.4 ist nach Herstellerangabe nicht betroffen. FortiSASE-Instanzen wurden von Fortinet bereits am 5. März 2024 zentral gepatcht.

Regulatorischer Hinweis: Ein bestätigter Zugriff auf den Management-Server oder ein Abfluss personenbezogener Daten 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

05.03.2024
Fortinet patcht die eigenen FortiSASE-Instanzen

März 2024
Fortinet veröffentlicht Advisory FG-IR-24-007, Fixes 7.2.3 / 7.0.11

21.03.2024
Horizon3.ai veröffentlicht technische Analyse und PoC-Exploit

25.03.2024
CISA nimmt CVE-2023-48788 in den KEV-Katalog auf – Frist 15.04.2024

Ihr Maßnahmenplan.

In dieser Reihenfolge – Zugriff einschränken, patchen, Kompromittierung ausschließen, Zugangsdaten rotieren.

SOFORT	KURZFRISTIG	PARALLEL
Netzzugriff auf Port 8013 einschränken / patchen	Auf RCE-Spuren prüfen, Zugangsdaten rotieren	Threat Hunting / Log-Auswertung

01 Betroffenheit feststellen

Prüfen, ob FortiClientEMS in einer Version zwischen `7.0.1` und `7.0.10` bzw. `7.2.0` und `7.2.2` im Einsatz und der Dienst-Port `8013` über das Netz erreichbar ist.

02 Sofort mitigieren (vor dem Patch)

Den Netzzugriff auf FortiClientEMS – insbesondere TCP-Port `8013` – strikt auf autorisierte Hosts und Netze begrenzen und die Erreichbarkeit aus dem Internet unterbinden.

03 Patchen

Auf `FortiClientEMS 7.2.3` bzw. `7.0.11` oder neuer aktualisieren. Damit ist die SQL-Injection geschlossen.

04 Kompromittierung ausschließen

Prüfen, ob der SQL-Server-Befehl `xp_cmdshell` aktiviert wurde – ein starkes Zeichen für eine bereits erfolgte Ausnutzung. Ein Patch entfernt keinen bereits eingerichteten Zugang.

```
SELECT value_in_use FROM
sys.configurations WHERE name =
'xp_cmdshell';
```

05 Spuren auswerten & Zugangsdaten rotieren

MS-SQL-Logs auf `xp_cmdshell`-Aufrufe und die EMS-Logs unter `C:\Program Files (x86)\Fortinet\FortiClientEMS\logs` auf fremde Verbindungen zu Port 8013 durchsuchen; im Verdachtsfall Dienst-, Datenbank- und Admin-Zugangsdaten rotieren.

Kompromittierungs-Indikatoren (IoCs)

KOMPROMITTIERUNGS-CHECK	AUFFÄLLIGE AKTIVITÄT	LOG-QUELLE
Aktivierung von `xp_cmdshell` auf dem Microsoft-SQL-Server (MSSQL-Logs)	Unerwartete Verbindungen fremder Clients zu `FmcDaemon` auf Port `8013`	`C:\Program Files (x86)\Fortinet\FortiClientEMS\logs` auf Anomalien prüfen

Zur Einordnung: Der zuverlässigste Hinweis auf eine erfolgte Ausnutzung ist die Aktivierung und Nutzung von xp_cmdshell in den SQL-Server-Logs. Da die Injection über reguläre Dienst-Anfragen an Port 8013 läuft, ist sie ohne detaillierte Verbindungs- und Datenbank-Logs schwer zu erkennen – Fortinet nennt im Advisory keine festen IoCs.

Wichtig: Die Gefahr endet nicht bei der Datenbank: Über xp_cmdshell wird aus der SQL-Injection eine vollständige Serverübernahme. Wurde die Lücke bereits ausgenutzt, kann ein hinterlassener Zugang auch nach dem Patch bestehen bleiben – deshalb ist die Prüfung auf Kompromittierung ebenso wichtig wie das Update.

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 Verbindungen zu FmcDaemon auf Port 8013 und die Aktivierung/Nutzung von xp_cmdshell auf dem SQL-Server fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte FortiClientEMS-Instanzen (Port 8013) 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 FortiClientEMS-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

- Netzzugriff auf FortiClientEMS (Port 8013) heute einschränken; Patch auf 7.2.3 / 7.0.11 unverzüglich einplanen.
- Prüfen lassen, ob xp_cmdshell aktiviert wurde und bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Im Verdachtsfall Dienst-, Datenbank- und Admin-Zugangsdaten rotieren lassen.

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-2023-48788 und dem FortiClientEMS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-24-007 (CVSS 3.1: 9,3; Fixes 7.2.3 / 7.0.11) · NVD CVE-2023-48788 (CVSS 3.1: 9,8 / KRITISCH, CWE-89, Vektor AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 25.03.2024, Frist 15.04.2024) · Horizon3.ai Attack Research (Deep-Dive + PoC). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.