AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-25257

Pre-Auth-SQL-Injection in Fortinet FortiWeb.

Ein nicht authentifizierter Angreifer aus dem Internet kann über den Fabric Connector von FortiWeb SQL-Befehle einschleusen und diese bis zur Codeausführung mit Root-Rechten eskalieren – ohne gültige Anmeldedaten. Betroffen ist jedes Gerät mit erreichbarem HTTP/HTTPS-Management-Interface; öffentliche Exploits kursieren, die Ausnutzung läuft seit Juli 2025.

> **Geschäftsrisiko:** vollständige Kompromittierung der Web Application Firewall – mit Potenzial für Umgehung des Schutzes dahinterliegender Anwendungen, Datenabfluss, Persistenz im Netz 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 – volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD-Basiswert 9,8 (CVSS 3.1); Fortinet nennt inkl. Temporal-Metriken 9,6. Eine CVSS-4.0-Bewertung liegt beim NVD nicht vor.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Juli 2025	FortiWeb 7.0 – 7.6 (HTTP/HTTPS-Management)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Pre-Auth-RCE
SQL-Injection über Fabric Connector

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

FortiWeb 6.4
& älter nicht betroffen

Die Ursache: Die Authentifizierungsfunktion des Fabric Connectors übernimmt den Token aus dem **Authorization**-Header ungeprüft in eine SQL-Abfrage – ein klassischer, unauthentifizierter SQL-Injection-Punkt. Über `INTO OUTFILE` lässt sich damit eine Python-Datei in das site-packages-Verzeichnis schreiben, die beim nächsten CGI-Aufruf ausgeführt wird. So wird aus der Datenbank-Injektion eine Codeausführung mit **Root-Rechten**.

ANGRIFFSKETTE

01
GUI exponiert – FortiWeb-Management-Interface (HTTP/HTTPS) ist aus dem Internet erreichbar

02
SQL einschleusen – gefälschter Authorization-Header an `/api/fabric/*`, Token landet ungefiltert in der DB-Abfrage

03
Datei schreiben – per `SELECT … INTO OUTFILE` eine Python-Datei ins site-packages-Verzeichnis schreiben

04
Root-Code – die untergeschobene Datei wird über CGI ausgeführt → Codeausführung als root

Betroffenheit & Fixversionen

FortiWeb-Zweig	Verwundbar bis	Fixversion (Ziel)
7.6	`7.6.0 – 7.6.3`	`7.6.4`
7.4	`7.4.0 – 7.4.7`	`7.4.8`
7.2	`7.2.0 – 7.2.10`	`7.2.11`
7.0	`7.0.0 – 7.0.10`	`7.0.11`
6.4 · älter	nicht betroffen	—

Praktisch angreifbar sind nur Geräte mit erreichbarem HTTP/HTTPS-Management-Interface. FortiWeb 6.4 und ältere Zweige sind laut Hersteller **nicht** betroffen. Exakte Build-Ranges gegen das Advisory FG-IR-25-151 abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff bzw. eine Codeausführung auf der WAF 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

08.07.2025
Fortinet veröffentlicht Advisory FG-IR-25-151 (CVSS 9,6)

18.07.2025
Fortinet meldet Ausnutzung in der Breite; CISA nimmt in KEV auf

08.08.2025
CISA-Frist für US-Bundesbehörden (BOD 22-01)

Seither
Öffentliche PoCs; fortlaufende Ausnutzung exponierter Interfaces

Ihr Maßnahmenplan.

In dieser Reihenfolge – Interface abschotten vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Management-Interface vom Internet trennen	Patch einspielen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

FortiWeb-Version prüfen (Zweige 7.0 bis 7.6). Ist das HTTP/HTTPS-Management-Interface aus dem Internet oder aus nicht vertrauenswürdigen Netzen erreichbar? Nur exponierte Interfaces sind praktisch angreifbar.

02 Sofort mitigieren (vor dem Patch)

Herstellerbehelf: den HTTP/HTTPS-Administrationszugang deaktivieren bzw. am exponierten Interface aus `allowaccess` entfernen und auf vertrauenswürdige Hosts / VPN beschränken:

```
config system interface edit <port> set allowaccess ping ssh next end
```

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`7.6.4` · `7.4.8` · `7.2.11` · `7.0.11` oder höher). Fortinet hat für alle betroffenen Zweige feste Builds veröffentlicht.

04 Kompromittierung ausschließen

Logs auf Fabric-API-Aufrufe mit SQL-Fragmenten sowie das Dateisystem auf neu angelegte `.pth`/`.py`-Dateien prüfen und die IoCs unten abgleichen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Root-Zugriff.

05 Perimeter härten

Grundsatz durchsetzen: Administrations-Interfaces nie direkt exponieren. Vorgelagerte WAF-/IPS-Signaturen für diese Schwachstelle einspielen, sofern verfügbar.

Kompromittierungs-Indikatoren (IoCs)

VERDÄCHTIGE AUFRUFE

POST auf `/api/fabric/device/status` und weitere `/api/fabric/*`-Endpunkte mit gefälschtem `Authorization`-Header

SQL-MARKER IN LOGS

SQL-Fragmente wie `UNION SELECT`, `INTO OUTFILE` · Datenbank-Fehlermeldungen

UNTERGESCHOBENE DATEIEN

neue `.pth` / `.py`-Dateien im Python-site-packages-Verzeichnis · Ausführung via CGI (`ml-draw.py`)

Zur Einordnung: Die genannten Endpunkte sind reguläre Fabric-Connector-Aufrufe – auffällig erst mit SQL-Payload im Authorization-Header. Datei- und Log-Marker sind eine Momentaufnahme der beobachteten Kampagne und kein Ersatz für die Analyse Ihrer Zugriffs- und Systemlogs.

Wichtig: Eine erfolgreiche Ausnutzung hinterlässt schreibenden Root-Zugriff auf dem Gerät. Ein reiner Patch entfernt bereits untergeschobene Dateien, Konten oder Persistenz nicht – ohne Prüfung des Systems bleibt eine erfolgte Kompromittierung 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: SQL-Injection-Muster in Fabric-API-Aufrufen und neu angelegte Dateien im Python-Verzeichnis fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte FortiWeb-Management-Interfaces 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 FortiWeb-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

- Management-Interface heute vom Internet trennen, Patch innerhalb der CISA-Frist (08.08.2025) einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Grundsatz durchsetzen: Administrations-Interfaces nie direkt exponieren.

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-2025-25257 und dem FortiWeb-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-25-151 (CVE-2025-25257) · NVD (nvd.nist.gov, CVSS 3.1 Basiswert 9,8) · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 18.07.2025, Frist 08.08.2025). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.