AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-64446

# Authentifizierungs-Bypass per Pfad-Traversal in Fortinet FortiWeb.

Ein nicht authentifizierter Angreifer aus dem Internet kann über eine manipulierte URL an der Authentifizierung des FortiWeb-Managements vorbei administrative Befehle absetzen – und sich damit ein eigenes Administrator-Konto auf der Appliance anlegen. Die Ausnutzung ist trivial, erfolgt mit einer einzigen HTTP-Anfrage und läuft nachweislich seit Anfang Oktober 2025.

> **Geschäftsrisiko:** vollständige Übernahme der Web Application Firewall – mit Potenzial zum Abschalten von Schutzregeln, Datenabfluss, Weiterbewegung ins interne Netz 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 Rechte, ohne Zutun – mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Fortinet weist den Basiswert 9,8 aus (mit Temporal-Metriken 9,4).

| AUSGENUTZT SEIT | BETROFFEN | HANDLUNGSBEDARF |
|---|---|---|
| 6. Oktober 2025 | FortiWeb 7.0 – 8.0.1 (GUI-Management aus dem Netz erreichbar) | Sofort |

# Das Wichtigste in 60 Sekunden.

**9,8 · KRITISCH**
CVSS-Schweregrad

**Auth-Bypass**
Neues Admin-Konto ohne Anmeldung

**Aktiv**
ausgenutzt · CISA KEV · PoC öffentlich

**6.4 & Cloud**
FortiWeb 6.4 und FortiAppSec Cloud nicht betroffen

**Die Ursache:** Die GUI des FortiWeb-Managements normalisiert eingehende URLs unzureichend. Über eine relative Pfad-Traversal (`?/../../../../../cgi-bin/fwbcgi`) lässt sich eine Anfrage an den internen CGI-Handler `fwbcgi` umleiten. In Verbindung mit einem selbstgesetzten, base64-kodierten CGIINFO-Header wird die Anfrage so verarbeitet, als käme sie mit interner Administrator-Autorisierung – die äußere Authentifizierung entfällt vollständig (CWE-23).

## ANGRIFFSKETTE

| 01 | 02 | 03 | 04 |
|---|---|---|---|
| **Management exponiert** – FortiWeb-GUI ist per HTTP/HTTPS aus dem Internet erreichbar | **Pfad-Traversal** – URL `/api/v2.0/cmdb/system/admin?/../../../../../cgi-bin/fwbcgi` leitet auf den internen Handler um | **Auth umgehen** – manipulierter `CGIINFO`-Header erzwingt interne Admin-Autorisierung | **Übernahme** – ein einziger POST legt ein neues Administrator-Konto an; Angreifer meldet sich regulär an |

## Betroffenheit & Fixversionen

| FortiWeb-Zweig | Verwundbar bis | Fixversion (Ziel) |
|---|---|---|
| 8.0 | `8.0.0 – 8.0.1` | `8.0.2` |
| 7.6 | `7.6.0 – 7.6.4` | `7.6.5` |
| 7.4 | `7.4.0 – 7.4.9` | `7.4.10` |
| 7.2 | `7.2.0 – 7.2.11` | `7.2.12` |
| 7.0 | `7.0.0 – 7.0.11` | `7.0.12` |
| 6.4 · FortiAppSec Cloud | nicht betroffen | — |

Betroffen sind alle Appliances der Zweige 7.0 bis 8.0 mit erreichbarer Management-GUI. Fortinet nennt die Fixversionen je Zweig verbindlich; exakte Build-Stände gegen das Hersteller-Advisory FG-IR-25-910 des eigenen Zweigs abgleichen. FortiWeb 6.4 und FortiAppSec-Cloud-Umgebungen sind laut Fortinet nicht angreifbar.

**Regulatorischer Hinweis:** Ein bestätigter unbefugter Admin-Zugriff auf die 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

06.10.2025 | 12.11.2025 | 14.11.2025 | 21.11.2025

# Ihr Maßnahmenplan.

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

| SOFORT | KURZFRISTIG | PARALLEL |
|---|---|---|
| Management vom Netz nehmen | Patch einspielen | Threat Hunting / IoC-Abgleich |

## 01 Exposition sofort beenden

Prüfen, ob die FortiWeb-Management-GUI aus dem Internet erreichbar ist. Fortinet empfiehlt als Sofortmaßnahme, HTTP/HTTPS auf allen internetseitigen Schnittstellen zu deaktivieren und den Zugriff auf das Management auf interne, vertrauenswürdige Netze zu beschränken.

## 02 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren: `8.0.2` · `7.6.5` · `7.4.10` · `7.2.12` · `7.0.12` (oder neuer). Ab Version 8.0.2 werden Ausnutzungsversuche mit HTTP 403 abgewiesen; der Fix beschränkt den Zugriff auf den internen Handler `fwbcgi`.

## 03 Kompromittierung ausschließen

Konfiguration und Audit-Logs auf unbekannte, seit Anfang Oktober 2025 angelegte Administrator-/lokale Konten mit `prof_admin`-Profil prüfen. Bekannte Angreifer-Kontennamen unten abgleichen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

## 04 Kompromittierte Appliance bereinigen

Bei Fund unbekannter Admin-Konten: Konten entfernen, Zugangsdaten und Zertifikate rotieren, Konfiguration auf manipulierte Regeln/Änderungen prüfen. Im Zweifel Neuaufsetzen aus einem sauberen Stand erwägen und Incident Response einbinden.

## 05 Dauerhaft absichern

Management-Interfaces grundsätzlich nicht ins Internet exponieren, sondern über VPN/Jump-Host erreichbar machen. Herstellerseitige Updates zeitnah einspielen und die Auth-Logs des Perimeters kontinuierlich auswerten.

## Kompromittierungs-Indikatoren (IoCs)

**EXPLOIT-MUSTER (URL)**

`/api/v2.0/cmdb/system/admin?/../../../../../cgi-bin/fwbcgi`

POST mit base64-kodiertem `CGIINFO`-Header

**NEU ANGELEGTE ADMIN-KONTEN**

Kontennamen `Testpoint`, `trader`, `trader1` (illustrativ auch `hax0r`) mit `prof_admin`-Profil

**ANGREIFER-HERKUNFT**

Anfragen aus den USA, Europa und Asien

Zeitraum ab `Anfang Oktober 2025`

**Zur Einordnung:** Die genutzten Kontennamen und Passwörter sind eine Momentaufnahme der beobachteten Kampagne und flüchtig – kein Ersatz für eine vollständige Prüfung aller Administrator-Konten und Audit-Logs. Der Erfolg zeigt sich vor allem an neuen, nicht autorisierten Admin-Konten seit Anfang Oktober 2025.

**Wichtig:** Ein erfolgreicher Angriff hinterlässt vor allem ein zusätzliches, regulär nutzbares Administrator-Konto – ohne Alarm. Ohne Prüfung der Konten- und Audit-Logs bleibt ein bereits erfolgter Zugriff unsichtbar, selbst nach dem Patch.

# 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: Die Anlage eines neuen Admin-Kontos und Pfad-Traversal-Anfragen an die Management-GUI fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

## Vulnerability & Exposure Management

Wir finden internetseitig exponierte, ungepatchte FortiWeb-Management-GUIs 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-Zugang heute vom Internet trennen, Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein unbefugtes Admin-Konto angelegt wurde – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung des Perimeters und der Management-Interfaces 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-2025-64446 und dem FortiWeb-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-25-910 · NIST NVD CVE-2025-64446 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 14.11.2025) · Rapid7 Emergent Threat Report · Bishop Fox / Qualys / Arctic Wolf Analysen. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.