AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-58034

OS-Command-Injection in Fortinet FortiWeb.

Ein authentifizierter Angreifer kann über präparierte HTTP-Anfragen oder CLI-Kommandos beliebige Betriebssystembefehle auf einer FortiWeb-Appliance ausführen – bis hin zur vollständigen Übernahme des Geräts. Fortinet beobachtet aktive Ausnutzung in freier Wildbahn; die Lücke wird häufig mit dem Authentifizierungs-Bypass CVE-2025-64446 verkettet, der die benötigten Rechte erst liefert.

> **Geschäftsrisiko:** vollständige Kompromittierung der Web-Application-Firewall am Perimeter – mit Potenzial für Datenabfluss, Manipulation des geschützten Datenverkehrs, Brückenkopf ins interne Netz und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

7,2 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz, ohne Zutun des Nutzers, aber mit hohen Rechten – mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Fortinet selbst bewertet mit temporalem Vektor 6,7 (aktiv ausgenutzt, Fix verfügbar).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
November 2025	FortiWeb 7.0 – 8.0.1 (6.4 nicht betroffen)	Sofort

Das Wichtigste in 60 Sekunden.

7,2 · HOCH
CVSS-Schweregrad (NVD)

OS-Command-Injection
beliebige Befehle auf der Appliance

Aktiv
ausgenutzt · CISA KEV · verkettet mit 64446

6.4 / FortiAppSec Cloud
nicht betroffen

Die Ursache: FortiWeb bereinigt Eingaben in einer Verwaltungsfunktion nicht ausreichend, bevor sie an eine Betriebssystem-Shell weitergereicht werden (CWE-78). Ein authentifizierter Angreifer kann so über präparierte HTTP-Anfragen oder CLI-Kommandos eigene Befehle in den zugrunde liegenden Kontext einschleusen und mit den Rechten der Appliance ausführen. In der Praxis wird die zunächst nötige Authentifizierung häufig über den parallelen Path-Traversal-/Auth-Bypass CVE-2025-64446 beschafft – die Kombination macht aus einer „Nur-für-Angemeldete"-Lücke einen faktisch vorauthentifizierungsfreien Angriffsweg.

ANGRIFFSKETTE

01	02	03	04
Management exponiert – FortiWeb-Verwaltungsoberfläche ist aus dem Netz erreichbar	**Rechte beschaffen** – Authentifizierung, oft über verketteten Bypass CVE-2025-64446	**Befehl einschleusen** – OS-Kommandos über präparierte HTTP-Anfrage oder CLI	**Übernahme** – Codeausführung im Appliance-Kontext, Persistenz und Zugang ins Netz

Betroffenheit & Fixversionen

FortiWeb-Zweig	Verwundbar bis	Fixversion (Ziel)
8.0	8.0.0 – 8.0.1	8.0.2
7.6	7.6.0 – 7.6.5	7.6.6
7.4	7.4.0 – 7.4.10	7.4.11
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	—

Fortinet nennt für jeden Zweig eine feste Fixversion („oder höher"). Exakte Build-Stände gegen das Hersteller-Advisory FG-IR-25-513 des eigenen Zweigs abgleichen. FortiWeb 6.4 sowie der Cloud-Dienst FortiAppSec Cloud sind laut Fortinet nicht betroffen.

Regulatorischer Hinweis: Eine bestätigte Kompromittierung der Perimeter-Firewall 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

14.11.2025 | 18.11.2025 | 18.11.2025 | 25.11.2025

Ihr Maßnahmenplan.

In dieser Reihenfolge – Perimeter abriegeln, patchen, dann Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Management-Zugang einschränken	Patch einspielen	Threat Hunting / Log-Analyse

01 Betroffenheit feststellen

FortiWeb-Version und -Zweig ermitteln und gegen die Fixversionen abgleichen. Prüfen, ob die Verwaltungsoberfläche (HTTP/HTTPS/SSH) aus nicht vertrauenswürdigen Netzen erreichbar ist – exponierte Management-Interfaces sind das primäre Angriffsziel.

02 Sofort abriegeln (vor dem Patch)

Zugriff auf die FortiWeb-Verwaltung strikt auf vertrauenswürdige Quell-IPs beschränken und aus dem Internet entfernen (trusthosts / lokale Policy). Da die Lücke oft mit dem Auth-Bypass CVE-2025-64446 verkettet wird, ist die Reduktion der Angriffsfläche am Management-Interface die wirksamste Sofortmaßnahme.

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`8.0.2` · `7.6.6` · `7.4.11` · `7.2.12` · `7.0.12` oder höher). Denselben Patch-Vorgang nutzen, um auch den verketteten Auth-Bypass CVE-2025-64446 zu schließen.

04 Kompromittierung ausschließen

Da vor dem Patch bereits eine Ausnutzung erfolgt sein kann: Konfiguration auf unerwartete Änderungen prüfen, neu angelegte oder veränderte Administrator-Konten kontrollieren, Logs auf ungewöhnliche CLI-/Systembefehle und unbekannte Prozesse durchsehen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Anmeldedaten und Zertifikate rotieren

Bei Verdacht auf Kompromittierung Administrator-Passwörter, API-Schlüssel und auf der Appliance hinterlegte Zertifikate/Geheimnisse erneuern – ein Angreifer mit Codeausführung konnte diese auslesen.

Kompromittierungs-Indikatoren (IoCs)

VERWALTUNGS-ENDPUNKTE

Unerwartete `POST`-Anfragen an die FortiWeb-Management-/API-Oberfläche auffällig in Verbindung mit dem Traversal-Muster aus `CVE-2025-64446`

VERHALTENSMARKER

Neu angelegte oder unerwartet privilegierte Admin-Konten
ungewöhnliche CLI-/Systembefehle, fremde Prozesse, geänderte Konfiguration

ZUGRIFFSQUELLEN

Verwaltungs-Logins von unbekannten oder externen Quell-IPs
Zugriffe außerhalb üblicher Wartungsfenster

Zur Einordnung: Zu dieser Schwachstelle sind zum Stand dieses Dokuments keine belastbaren, herstellerbestätigten Netz-IoCs (feste Angreifer-IPs oder Datei-Hashes) öffentlich – die genannten Punkte sind Verhaltensindikatoren. Maßgeblich ist die Auswertung Ihrer eigenen FortiWeb-Admin-, System- und Zugriffs-Logs; verketten Sie die Analyse mit den IoCs zu CVE-2025-64446.

Wichtig: Der Angriff setzt Authentifizierung voraus – in der beobachteten Praxis wird diese jedoch über den verketteten Bypass CVE-2025-64446 beschafft, sodass der Schutz durch „nur für Angemeldete“ in der Realität nicht trägt. Beide CVEs zusammen behandeln.

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: Unerwartete Admin-Aktivität und anomale Systembefehle auf der FortiWeb-Appliance fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Netz erreichbare, ungepatchte FortiWeb-Verwaltungsoberflächen 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 abriegeln, Patch für beide verketteten CVEs innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung exponierter Sicherheits-Appliances 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-2025-58034 und dem FortiWeb-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-25-513 (CVE-2025-58034) · NVD (CVSS 3.1 Basiswert 7,2) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 18.11.2025, Frist 25.11.2025) · Fortinet-Advisory FG-IR-25-910/CVE-2025-64446 (verkettete Schwachstelle). 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.