

PREPARE **PROTECT** DETECT RESPOND IMPROVE

● AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-61624

Path Traversal in der FortiOS-CLI: vom Admin-Konto zu Root auf der Firewall.

In der Kommandozeile von FortiOS, FortiProxy, FortiPAM und FortiSwitchManager prüft Fortinet Dateinamen in bestimmten Befehlen unzureichend: Wer bereits ein Admin-Konto mit Schreibrechten besitzt, kann per Verzeichniswechsel beliebige Dateien schreiben oder löschen – und so auf Root-Ebene ausbrechen. Fixes gibt es seit April 2026; im Oktober dokumentierte Unit 42 die Ausnutzung für ein verdecktes Implantat, CISA nahm die Lücke am 16. Oktober in den KEV-Katalog auf – mit forensischer Triage-Pflicht.

Geschäftsrisiko: kein Einstiegspunkt, sondern ein Verstärker: Wer schon Admin-Zugang hat, setzt ein dauerhaftes, schwer erkennbares Implantat, liest Datenverkehr mit und umgeht VPN-Kontrollen – dann ist ein meldepflichtiger Vorfall nach NIS-2 / DSGVO wahrscheinlich.

6,5 / 10

MITTEL

CVSS 3.1 BASISWERT



CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H – über das Netz, aber nur mit angemeldetem Admin-Konto (Schreibrechte), ohne Zutun eines Nutzers, hohe Wirkung auf Integrität und Verfügbarkeit. Basiswert der NVD; Fortinet als CNA bewertet lokal (AV:L) mit 6,0, inkl. Temporal-Metriken 5,4.

AUSGENUTZT SEIT

spätestens 14.10.2026 (Unit 42)

BETROFFEN

FortiOS · FortiProxy · FortiPAM · FSM
Fix: FortiOS 7.6.5 · 7.4.10

HANDLUNGSBEDARF

Zeitnah

Das Wichtigste in 60 Sekunden.

6,5 · MITTEL

CVSS 3.1 (NVD) · Fortinet: 6,0

Admin nötig

Schreibrechte · CLI · Rechteauserweiterung zu Root

Aktiv

ausgenutzt · CISA KEV · Frist 19.10.2026

Patch da

FortiOS 7.6.5 · 7.4.10 · Zweige ≤ 7.2 migrieren



Die Ursache: FortiOS-Administratoren – auch ein **super_admin** – arbeiten in einer eingeschränkten Kommandozeile ohne Shell; die Dienste darunter laufen als Root. In bestimmten CLI-Befehlen prüft FortiOS nicht, ob übergebene Namen im vorgesehenen Verzeichnis bleiben (**CWE-22**) – laut Unit 42 etwa beim Objektnamen in `config system auto-script`: Ein Name mit `../` legt den Inhalt an beliebiger Stelle ab. Mit **Admin-Profil und Schreibrechten** erreicht ein Angreifer so Codeausführung als Root. **Ohne gültiges Admin-Konto ist die Lücke nicht ausnutzbar** – sie verlängert einen bereits erfolgten Einbruch.

ANGRIFFSKETTE

01

Admin-Zugang – gestohlene Zugangsdaten oder vorgelagerte Lücke, z. B. über FortiManager

02

Präparierter CLI-Befehl – Auto-Script mit `../` im Namen verlässt das Zielverzeichnis

03

Datei als Root geschrieben – Loader oder manipulierte Dienstkonfiguration abgelegt

04

Verdecktes Implantat – Mitschnitt, VPN-Umgehung, dauerhafter Zugang

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.6 / 7.4	7.6.0 – 7.6.4 · 7.4.0 – 7.4.9	7.6.5 · 7.4.10
FortiOS 7.2 / 7.0 / 6.4	alle Versionen	Migration auf gefixten Zweig
FortiProxy 7.6 / 7.4	7.6.0 – 7.6.4 · 7.4.0 – 7.4.11	7.6.5 · 7.4.12 (7.2/7.0: migrieren)
FortiPAM	1.0 – 1.7.0	1.7.1 · 1.8 nicht betroffen
FortiSwitchManager	7.2.0 – 7.2.7 · 7.0.0 – 7.0.6	7.2.8 · 7.0.7

Fixes seit FG-IR-26-122 vom 14.04.2026. Für FortiOS 7.2/7.0/6.4, FortiProxy 7.2/7.0 und FortiPAM 1.0–1.6 gibt es **keinen Fix im eigenen Zweig** – nur Migration. FortiSASE ist serverseitig behoben. Maßgeblich ist das Hersteller-Advisory.



Regulatorischer Hinweis: Ein Implantat auf der Firewall mit Zugriff auf Datenverkehr und VPN-Zugänge ist in der Regel meldepflichtig – 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 Forensik.

ZEITACHSE

ab 09/2024

Intrusion beginnt (Unit 42)

14.04.2026

FG-IR-26-122 mit Fixes

14.10.2026

Unit 42: Implantat PEERSTITCH

16.10.2026

CISA-KEV · Frist 19.10.2026

CVE-2025-61624 · Überblick

Seite 3: Ihr Maßnahmenplan →

Ihr Maßnahmenplan.

In dieser Reihenfolge – Admin-Zugänge härten, zügig patchen, Prüfung vor Entwarnung.

SOFORT

Admin-Zugänge prüfen und einschränken

KURZFRISTIG

Auf FortiOS 7.6.5 / 7.4.10 aktualisieren

PARALLEL

Auto-Scripts und Dateisystem prüfen

01

Betroffenheit feststellen

Firmware-Stand aller FortiGate-, FortiProxy-, FortiPAM- und FortiSwitchManager-Instanzen erheben. Geräte auf FortiOS 7.2, 7.0 oder 6.4 sind ohne Migration nicht zu beheben.

02

Admin-Zugänge härten (vor dem Patch)

Die Lücke braucht ein Admin-Konto mit Schreibrechten. Admin-Konten und Profile auf das Nötige reduzieren, MFA erzwingen, Verwaltungszugriff per Trusted Hosts auf Admin-Netze begrenzen und Zugangsdaten rotieren, falls Konfigurationen oder ein FortiManager kompromittiert waren.

03

Patchen

Auf FortiOS 7.6.5 · 7.4.10 bzw. die Fixstände für FortiProxy, FortiPAM und FortiSwitchManager aktualisieren; Zweige ohne Fix als Migration einplanen. Fortinet bietet zusätzlich einen virtuellen Patch (FG-VD-59270.0day, FMWP 25.120).

04

Kompromittierung ausschließen

Der Patch entfernt kein bereits gesetztes Implantat. Konfiguration auf Auto-Script-Objekte mit ../ im Namen prüfen, Admin-Logs auf deren Anlage sichten, nach fremden Dateien unter /data2/template/ suchen. CISA verlangt eine forensische Triage.

05

Bei Verdacht: Gerät als kompromittiert behandeln

Beweise sichern, Gerät aus vertrauenswürdiger Firmware neu aufsetzen, alle Admin-, VPN- und Dienstzugänge sowie Zertifikate erneuern.

Q Kompromittierungs-Indikatoren (IoCs)

ANGREIFER-IP-ADRESSEN

23.240.77.233
47.18.167.159

DATEIARTEFAKTE

In /data2/template/:lldprx,
ipsem.js,
index.js, index.wasm; fremde md-
acme.conf

LOG-/KONFIG-HINWEISE

Auto-Script-Objekte mit ../ im Namen,
z. B. ../ ../ ../ ../ setup; SSL-VPN-
Logins
von unbekannter Infrastruktur

Zur Einordnung: Die Indikatoren stammen aus einer einzelnen Incident-Analyse von Unit 42 (Cluster CL-STA-0954); Fortinet selbst veröffentlicht keine IoCs. Das Implantat arbeitet im Arbeitsspeicher und ist leicht anpassbar – belastbarer als die Suche nach einzelnen Indikatoren ist die Prüfung der Auto-Script-Objekte und der Frage, wer wann mit Schreibrechten angemeldet war.



Wichtig: Diese Lücke öffnet keine Tür – sie macht aus einem bereits erbeuteten Admin-Zugang eine dauerhafte, kaum sichtbare Kontrolle über die Firewall. Wer nur patcht, ohne Admin-Zugänge und Auto-Scripts zu prüfen, übersieht genau diesen Fall.

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: Neue Auto-Script-Objekte und Admin-Anmeldungen mit Schreibrechten ohne Change sowie unerwartete Prozesse oder Dateien auf der Firewall fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.



Vulnerability & Exposure Management

Wir finden FortiGate-, FortiProxy-, FortiPAM- und FortiSwitchManager-Instanzen mit vielen oder extern erreichbaren Admin-Zugängen 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 FortiOS-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

- › Diese Woche anordnen: Admin-Zugänge zu Fortinet-Geräten auf das Nötige reduzieren, MFA erzwingen und die Verwaltung auf Admin-Netze beschränken.
- › Fixversion zügig einspielen; Geräte auf FortiOS 7.2 und älter als Migrationsprojekt mit Termin aufsetzen.
- › Für Geräte mit Verdacht auf frühere Kompromittierung – etwa über FortiManager – eine forensische Prüfung beauftragen, dokumentiert für eine etwaige Meldung.

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-2025-61624 und dem FortiOS-Perimeter.

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



Termin buchen