AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-68686

Patch-Bypass in FortiOS: Symlink-Persistenz lebt weiter.

Fortinet hatte 2025 einen Angreifer-Trick entschärft, mit dem sich Zugriff auf FortiGate-Firewalls über einen versteckten Symlink dauerhaft halten ließ. Dieser Patch prüfte den Anfragepfad nur als Zeichenkette – ein zusätzlicher Schrägstrich genügt, um ihn zu umgehen. Wer irgendwann über eine ältere SSL-VPN-Lücke kompromittiert wurde, kann trotz aller Updates weiter unbemerkt ausgelesen werden. Die Schwachstelle steht seit dem 27. Juli 2026 im CISA-Katalog aktiv ausgenutzter Schwachstellen.

> **Geschäftsrisiko:** unbemerkter Abfluss der Firewall-Konfiguration – inklusive Regelwerk, VPN-Einstellungen und Passwort-Hashes – als Grundlage für einen zweiten, gezielten Angriff; mit Potenzial für einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

5,9 / 10

MITTEL
CVSS 3.1 BASISWERT

Niedrig | **Mittel** | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N` – aus dem Netz, ohne Rechte, ohne Zutun eines Nutzers, mit hoher Wirkung auf die Vertraulichkeit; die erhöhte Angriffskomplexität (AC:H) bildet die Voraussetzung einer bereits erfolgten Kompromittierung ab und drückt den Wert. Der Basiswert 5,9 stammt von Fortinet als CNA und steht so im NVD; die FortiGuard-Advisory-Seite nennt zusätzlich 5,3 als Wert mit Temporal-Metriken. Der moderate Zahlenwert täuscht über die Tragweite hinweg: Betroffen ist, wer bereits einmal kompromittiert wurde.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Juli 2026	FortiOS 6.4 – 7.6.1 nur mit aktivem SSL-VPN	Sofort prüfen

Das Wichtigste in 60 Sekunden.

5,9 · MITTEL
CVSS-Basiswert (NVD)

Patch-Bypass
Symlink-Persistenz im SSL-VPN

Aktiv
ausgenutzt · CISA KEV · Frist 10.08.2026

Ohne SSL-VPN
nicht betroffen

Die Ursache: Im April 2025 machte Fortinet öffentlich, dass Angreifer nach einer Erstkompromittierung im Ordner für die SSL-VPN-Sprachdateien einen **symbolischen Link auf das Root-Dateisystem** hinterlegten. Der Link überlebte jedes Firmware-Update und lieferte weiterhin lesenden Zugriff auf Gerätedateien. Der damalige Patch filterte Anfragen, indem er im Pfad nach der Zeichenkette `/lang/custom` suchte – eine reine Textprüfung ohne Pfad-Normalisierung. Ein zusätzlicher Schrägstrich (`/lang//custom`) läuft an dieser Prüfung vorbei, während der Webserver den Pfad identisch auflöst. Ergebnis: Der alte Persistenz-Weg ist wieder offen.

ANGRIFFSKETTE

01
Altlast – Gerät wurde früher über eine SSL-VPN-Lücke auf Dateisystemebene übernommen

02
Symlink – Angreifer verlinkt den Sprachdatei-Ordner auf das Root-Dateisystem

03
Bypass – Anfrage mit doppeltem Schrägstrich umgeht die Zeichenketten-Prüfung

04
Auslesen – unauthentifizierter Lesezugriff auf Dateien inkl. Konfiguration

Betroffenheit & Fixversionen

FortiOS-Zweig	Verwundbar bis	Fixversion (Ziel)
7.6	`7.6.0 – 7.6.1`	`7.6.2 oder höher`
7.4	`7.4.0 – 7.4.6`	`7.4.7 oder höher`
7.2	alle Versionen	Migration auf 7.4.7 / 7.6.2
7.0	alle Versionen	Migration auf 7.4.7 / 7.6.2
6.4	alle Versionen	Migration auf 7.4.7 / 7.6.2
SSL-VPN deaktiviert	nicht betroffen	—

Fortinet stellt für die Zweige 7.2, 7.0 und 6.4 **keinen** eigenen Fix bereit – hier ist der Wechsel auf einen gefixten Zweig der einzige Weg. Geräte ohne aktivierten SSL-VPN-Dienst sind nicht betroffen. Exakte Build-Stände gegen FG-IR-25-934 abgleichen.

Regulatorischer Hinweis: Bestätigt sich ein unbefugter Zugriff auf die Konfiguration, kann darin eine meldepflichtige Verletzung liegen – 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

10.04.2025
Fortinet macht die Symlink-Persistenz öffentlich

26.04.2025
Bypass von ITRES Labs entdeckt, 09.10.2025 an Fortinet gemeldet

10.02.2026
Fortinet veröffentlicht FG-IR-25-934 und den korrigierten Patch

27.07.2026
Aufnahme in den CISA-KEV-Katalog · Behördenfrist 10.08.2026

Ihr Maßnahmenplan.

In dieser Reihenfolge – Betroffenheit vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
SSL-VPN-Status und Firmware prüfen	Auf 7.4.7 / 7.6.2 aktualisieren	Altkompromittierung ausschließen

01 Betroffenheit feststellen

Prüfen, ob der SSL-VPN-Dienst (Web-Modus oder Tunnel-Modus) aktiviert ist – ohne ihn besteht kein Risiko. Anschließend den Firmware-Stand jeder FortiGate erheben; betroffen sind alle Builds unterhalb 7.4.7 bzw. 7.6.2 sowie sämtliche Versionen der Zweige 7.2, 7.0 und 6.4.

```
get system status
```

02 Patchen bzw. Zweig wechseln

Auf `7.6.2` oder `7.4.7` (bzw. höher) aktualisieren. Für 7.2, 7.0 und 6.4 gibt es keinen Fix im eigenen Zweig – hier ist die Migration auf einen unterstützten Zweig erforderlich und ohnehin überfällig. Vorher Konfigurationssicherung ziehen.

03 Symlink-Altlast ausschließen

Der Patch schließt den Weg – er beweist nicht, dass niemand ihn genutzt hat. Prüfen, ob das Gerät jemals über eine der bekannten SSL-VPN-Lücken angreifbar war (CVE-2022-42475, CVE-2023-27997, CVE-2024-21762) und die von Fortinet bereitgestellten AV-/IPS-Signaturen zur Erkennung und Entfernung des Symlinks einspielen.

04 Konfiguration als kompromittiert behandeln

Bei jedem Verdacht auf einen früheren Zugriff gilt die gesamte Gerätekonfiguration als offengelegt: alle lokalen Admin- und VPN-Zugangsdaten sowie Pre-Shared Keys und Zertifikate erneuern, Regelwerk auf unbekannte Einträge prüfen. Ein Passwortwechsel nach dem Patch schützt nicht rückwirkend.

05 Übergangsweise virtuell patchen

Solange ein Update nicht möglich ist, bietet Fortinet ein virtuelles Patching über die FMWP-Datenbank (Signatur `FG-VD-60389.0day`, Update 26.033) an. Das ist ein Behelf, kein Ersatz für die Firmware-Aktualisierung. Zusätzlich den SSL-VPN-Zugang auf benötigte Quellen einschränken.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGES ANFRAGEMUSTER

Pfade mit doppeltem Schrägstrich, etwa `/lang//custom` statt `/lang/custom`

WO SUCHEN

Webserver-/Reverse-Proxy- und WAF-Logs vor der FortiGate, SSL-VPN-Zugriffe ohne zugehörige Anmeldung

VORGESCHICHTE PRÜFEN

Frühere Betroffenheit durch `CVE-2022-42475` · `CVE-2023-27997` · `CVE-2024-21762`

Zur Einordnung: Das Pfadmuster stammt aus der Veröffentlichung des Entdeckers (ITRES Labs) und ist von Fortinet nicht als offizieller Indikator bestätigt; es ist zudem trivial abwandelbar. Aussagekräftiger als die Suche nach einer Zeichenkette ist die Frage, ob das Gerät jemals über eine der genannten SSL-VPN-Lücken erreichbar war.

Wichtig: Der Zugriff ist rein lesend und hinterlässt keinen Anmeldevorgang – es gibt keinen fehlgeschlagenen Login, keinen Alarm, keine Sitzung. Wer nur auf Authentifizierungs-Ereignisse schaut, sieht diesen Abfluss nicht.

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: Anfragen an die SSL-VPN-Sprachdatei-Pfade ohne zugehörige Anmeldung fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Internet erreichbare FortiGate-SSL-VPN-Dienste 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

- Firmware-Stand aller FortiGate-Systeme diese Woche erheben und Update terminieren.
- Für Geräte auf 7.2, 7.0 oder 6.4 den Zweigwechsel als Projekt aufsetzen – dort endet der Support.
- Prüfen lassen, ob ein früherer Zugriff stattgefunden hat, und das Ergebnis für eine etwaige Meldung dokumentieren.

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-2025-68686 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-25-934 · NVD CVE-2025-68686 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 27.07.2026) · Fortinet PSIRT-Blog „Analysis of Threat Actor Activity" vom 10.04.2025 · ITRES Labs, Offenlegung des Bypasses vom 11.02.2026. Angaben nach bestem Wissen zum Stand 03.08.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.