AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2022-42475

Pre-Auth Remote Code Execution in Fortinet FortiOS SSL-VPN.

Ein nicht authentifizierter Angreifer aus dem Netz kann über einen Heap-basierten Pufferüberlauf im SSL-VPN von FortiOS und FortiProxy beliebigen Code auf der Firewall ausführen – ohne gültige Zugangsdaten und ohne Zutun eines Nutzers. Die Schwachstelle wurde bereits als Zero-Day aktiv ausgenutzt, bevor Fortinet den Patch am 12. Dezember 2022 veröffentlichte, und wird seither in gezielten Angriffen sowie in Verbindung mit persistenten Backdoors eingesetzt.

> **Geschäftsrisiko:** Vollständige Übernahme der Perimeter-Firewall durch einen unauthentifizierten Angreifer, dauerhafter Zugang zum internen Netz über hinterlegte Backdoors und Manipulation von Konfiguration und Logs – mit Potenzial für Datenabfluss, Ransomware, Betriebsunterbrechung 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 des Nutzers – vollständige Kompromittierung des Geräts mit Ausführung beliebigen Codes auf der Firewall. Fortinet selbst bewertet die Lücke mit CVSS 9,3.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Dezember 2022 (Zero-Day)	FortiOS ≤ 7.2.2 · FortiProxy ≤ 7.2.1 (SSL-VPN aktiviert)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1, NVD)

Pre-Auth RCE
ohne Anmeldung aus dem Netz

Zero-Day
aktiv ausgenutzt · CISA KEV (seit 13.12.2022)

CWE-787
Heap-Buffer-Overflow

Die Ursache: Der SSL-VPN-Dienst `sslvpnd` von FortiOS und FortiProxy verarbeitet speziell präparierte Anfragen fehlerhaft: Eine numerische Trunkierung führt dazu, dass zu viele Daten in einen zu klein bemessenen Speicherbereich auf dem Heap geschrieben werden (**Heap-based Buffer Overflow**). Ein **nicht authentifizierter** Angreifer kann diesen Überlauf über das offene VPN-Web-Interface auslösen und so beliebigen Code mit den Rechten des Dienstes auf der Firewall ausführen.

ANGRIFFSKETTE

01	02	03	04
SSL-VPN exponiert – das VPN-Web-Interface ist über das Internet erreichbar (typisch TCP/443)	**Präparierte Anfrage** – manipulierte, unauthentifizierte Anfrage löst den Heap-Überlauf im Dienst `sslvpnd` aus	**Codeausführung** – der Angreifer führt beliebigen Code auf der Firewall aus, ohne Zugangsdaten	**Persistenz & Ausweitung** – Nachladen von Backdoors, Manipulation von Konfiguration und Logs, Zugriff auf das interne Netz

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.2	`7.2.0 – 7.2.2`	`7.2.3`
FortiOS 7.0	`7.0.0 – 7.0.8`	`7.0.9`
FortiOS 6.4	`6.4.0 – 6.4.10`	`6.4.11`
FortiOS 6.2	`6.2.0 – 6.2.11`	`6.2.12`
FortiOS 6.0	`6.0.0 – 6.0.15`	`6.0.16`
FortiOS 5.x	`5.0 – 5.6 (alle)`	auf 6.4.11+ migrieren
FortiProxy 7.2 / 7.0 / 2.0	`≤ 7.2.1 / ≤ 7.0.7 / ≤ 2.0.11`	`7.2.2 / 7.0.8 / 2.0.12`

Verwundbar sind ausschließlich Geräte mit **aktiviertem SSL-VPN**. FortiProxy sowie die 6K/7K-Modelle (FortiOS-6K7K) sind ebenfalls betroffen und in eigenen Zweigen zu patchen. FortiOS 5.x erhält keinen Fix mehr und muss auf eine unterstützte, gepatchte Version migriert werden. Ist SSL-VPN nicht im Einsatz, besteht über diese Lücke kein direkter Angriffsweg – die Prüfung der Konfiguration ist trotzdem geboten.

Regulatorischer Hinweis: Eine bestätigte Kompromittierung der Perimeter-Firewall oder ein Abfluss personenbezogener Daten 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.

Ihr Maßnahmenplan.

In dieser Reihenfolge – exponierte VPNs prüfen, patchen, auf Kompromittierung untersuchen, Zugangsdaten rotieren.

SOFORT	KURZFRISTIG	PARALLEL
SSL-VPN-Exposition prüfen / patchen	IoC-Abgleich & Kompromittierungs-	Zugangsdaten & Zertifikate rotieren

01 Betroffenheit feststellen

Prüfen, ob FortiOS- oder FortiProxy-Geräte mit **aktiviertem SSL-VPN** in einer der betroffenen Versionen im Einsatz und über das Internet erreichbar sind. Auch 6K/7K-Modelle und ältere 5.x-Geräte einbeziehen.

02 Sofort mitigieren (vor dem Patch)

Ist ein sofortiger Patch nicht möglich, das SSL-VPN abschalten oder den Netzzugriff strikt auf autorisierte Quellen begrenzen. Von Fortinet als Behelfsmaßnahme benannt.

03 Patchen

Auf die feste Version des jeweiligen Zweigs aktualisieren – z. B. `FortiOS 7.2.3`, `7.0.9`, `6.4.11`, `6.2.12` oder `6.0.16`. Nicht mehr unterstützte 5.x-Geräte auf eine gepatchte Version migrieren.

04 Auf Kompromittierung prüfen

Die von Fortinet genannten IoC abgleichen: verdächtige Dateien im Dateisystem, bekannte Angreifer-IPs in den Logs und Crash-Einträge des SSL-VPN-Dienstes. Ein Patch entfernt keine bereits platzierte Backdoor.

```
grep -i 'sslvpnd' crashlog | grep
'Signal 11'
```

05 Zugangsdaten als kompromittiert behandeln

Bei Anzeichen einer Kompromittierung alle lokalen und angebundenen Zugangsdaten, VPN-Benutzerpasswörter, Admin-Konten sowie eingesetzte Zertifikate rotieren und die Konfiguration gegen eine bekannte, saubere Sicherung abgleichen.

Kompromittierungs-Indikatoren (IoCs)

VERDÄCHTIGE DATEIEN

`/data/lib/libips.bak`, `libgif.so`, `libiptcp.so`, `libipudp.so`, `libjepg.so`, `/data/etc/wxd.conf`, `/var/.sslvpnconfigbk`

CRASH-LOG-SIGNATUR

`application:sslvpnd … Signal 11 received, Backtrace` im FortiOS-Crashlog

BEKANNTE ANGREIFER-IPS

188.34.130.40, 103.131.189.143, 193.36.119.61, 172.247.168.153, 139.180.184.197 u. a.

Zur Einordnung: Die genannten Dateipfade, IPs und Crash-Log-Signaturen stammen aus dem Fortinet-Advisory FG-IR-22-398 und dokumentieren beobachtete Angriffe – ihr Fehlen schließt eine Kompromittierung nicht aus. Der zuverlässigste Nachweis ist eine forensische Prüfung von Dateisystem, Konfiguration und Logs gegen einen bekannten sauberen Stand.

Wichtig: Der Kern des Risikos liegt in der Persistenz: Angreifer haben diese Lücke genutzt, um dauerhafte Backdoors auf der Firewall zu hinterlegen und Konfiguration wie Logs zu manipulieren. Ein Patch schließt die Schwachstelle, entfernt aber keinen bereits erlangten Zugang. Deshalb ist die Prüfung auf Kompromittierung ebenso wichtig wie das Update.

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: Crash-Einträge des SSL-VPN-Dienstes, Verbindungen zu bekannten Angreifer-IPs und verdächtige Dateien auf FortiOS-Geräten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden über das Internet erreichbare FortiOS-/FortiProxy-Geräte mit aktivem SSL-VPN 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 SSL-VPN-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

- Alle SSL-VPN-fähigen Fortinet-Geräte heute auf die feste Version patchen oder das SSL-VPN vorübergehend abschalten.
- Betroffene Geräte gegen die Fortinet-IoC prüfen lassen und bei Verdacht eine forensische Untersuchung einleiten.
- Bei Kompromittierungshinweisen Zugangsdaten und Zertifikate rotieren und den Vorfall 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-2022-42475 und dem FortiOS SSL-VPN-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-22-398 (veröffentlicht 12.12.2022, Fortinet-CVSS 9,3) · NVD CVE-2022-42475 (CVSS 3.1: 9,8 KRITISCH, Vektor AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, CWE-787 / CWE-197) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 13.12.2022, Frist 03.01.2023). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.