AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-21762

Pre-Auth-RCE im SSL-VPN von Fortinet FortiOS.

Ein nicht authentifizierter Angreifer aus dem Internet kann über den SSL-VPN-Dienst (sslvpnd) von FortiOS mit speziell präparierten HTTP-Anfragen einen Speicherfehler auslösen und darüber beliebigen Code ausführen – ohne gültige Anmeldedaten. Betroffen ist jedes Gerät mit aktiviertem, erreichbarem SSL-VPN; öffentliche Exploits kursieren, und die Schwachstelle wird nachweislich ausgenutzt – auch in Ransomware-Kampagnen.

> **Geschäftsrisiko:** vollständige Kompromittierung der Firewall am Netzwerk-Perimeter – mit Potenzial für Umgehung des Perimeterschutzes, Zugriff auf das interne Netz, Datenabfluss, Persistenz 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 – volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD-Basiswert 9,8 (CVSS 3.1); Fortinet nennt inkl. Temporal-Metriken 9,6. Eine CVSS-4.0-Bewertung liegt beim NVD nicht vor.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Februar 2024	FortiOS 6.0 – 7.4 · FortiProxy 1.0 – 7.4 (SSL-VPN aktiviert)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Pre-Auth-RCE
Out-of-bounds-Write im SSL-VPN (sslvpnd)

Aktiv
ausgenutzt · CISA KEV · Ransomware-Nutzung

SSL-VPN aus
nicht erreichbar = nicht angreifbar

Die Ursache: Der SSL-VPN-Web-Daemon `sslvpnd` verarbeitet speziell präparierte HTTP-Anfragen fehlerhaft und schreibt dabei über die Grenzen eines vorgesehenen Speicherbereichs hinaus (Out-of-bounds Write, CWE-787). Öffentliche Analysen führen den Fehler auf die Verarbeitung von HTTP-Anfragen mit `chunked`-Transfer-Encoding zurück. Ein nicht authentifizierter Angreifer kann diesen Speicherfehler kontrolliert auslösen und so beliebigen Code auf dem Gerät ausführen – noch vor jeder Anmeldung.

ANGRIFFSKETTE

01 **SSL-VPN exponiert** – der SSL-VPN-Dienst von FortiOS ist aus dem Internet erreichbar

02 **Anfrage präparieren** – speziell geformte HTTP-Anfrage (u. a. via `chunked`-Encoding) an `sslvpnd`

03 **Speicher überschreiben** – die Anfrage löst einen Out-of-bounds-Write über den Puffer hinaus aus

04 **Code-Ausführung** – der kontrollierte Speicherfehler mündet in Codeausführung ohne Anmeldung

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.4	7.4.0 – 7.4.2	7.4.3
FortiOS 7.2	7.2.0 – 7.2.6	7.2.7
FortiOS 7.0	7.0.0 – 7.0.13	7.0.14
FortiOS 6.4	6.4.0 – 6.4.14	6.4.15
FortiOS 6.2	6.2.0 – 6.2.15	6.2.16
FortiOS 6.0	6.0.0 – 6.0.17	6.0.18
FortiProxy 7.4	7.4.0 – 7.4.2	7.4.3
FortiProxy 7.2	7.2.0 – 7.2.8	7.2.9
FortiProxy 7.0	7.0.0 – 7.0.14	7.0.15
FortiProxy 2.0	2.0.0 – 2.0.13	2.0.14
FortiProxy 1.2 · 1.1 · 1.0	alle Versionen	auf gepatchten Zweig migrieren

Praktisch angreifbar sind nur Geräte mit aktiviertem und erreichbarem SSL-VPN. FortiProxy 1.0 bis 1.2 erhalten keinen Fix im eigenen Zweig – hier ist eine Migration auf einen gepatchten Release nötig. Exakte Build-Ranges gegen das Advisory FG-IR-24-015 abgleichen.

Ihr Maßnahmenplan.

In dieser Reihenfolge – SSL-VPN abschalten oder abschotten vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

FortiOS-/FortiProxy-Version prüfen (FortiOS-Zweige 6.0 bis 7.4, FortiProxy 1.0 bis 7.4). Ist der SSL-VPN-Dienst aktiviert und aus dem Internet oder aus nicht vertrauenswürdigen Netzen erreichbar? Nur Geräte mit aktivem, erreichbarem SSL-VPN sind praktisch angreifbar.

02 Sofort mitigieren (vor dem Patch)

Herstellerbehelf: den SSL-VPN-Dienst deaktivieren. Wichtig – das bloße Abschalten von `web-mode` ist laut Fortinet **kein** gültiger Workaround. Wo SSL-VPN unverzichtbar ist, den Zugang auf vertrauenswürdige Quellen / dedizierte Interfaces einschränken:

```
config vpn ssl settings set status
disable end
```

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`FortiOS 7.4.3 · 7.2.7 · 7.0.14 · 6.4.15 · 6.2.16 · 6.0.18` oder höher; `FortiProxy 7.4.3 · 7.2.9 · 7.0.15 · 2.0.14`). FortiProxy 1.0 bis 1.2 auf einen gepatchten Release migrieren.

04 Kompromittierung ausschließen

Angesichts der aktiven Ausnutzung das Gerät als potenziell kompromittiert behandeln: SSL-VPN-Logs, Administratorkonten, Konfigurations- und Skript-Änderungen sowie ausgehende Verbindungen prüfen und die IoCs unten abgleichen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Perimeter härten

Grundsatz durchsetzen: Fernzugangs-Dienste nie ungeschützt exponieren, SSL-VPN nur wo nötig und mit MFA. Vorgelagerte IPS-Signaturen für diese Schwachstelle einspielen, sofern verfügbar.

Kompromittierungs-Indikatoren (IoCs)

VERDÄCHTIGE ANFRAGEN

präparierte HTTP-Anfragen an den SSL-VPN-Dienst (`/remote/*`) mit auffälligem `chunked`-Transfer-Encoding oder abgeschnittenen Anfragen

PROZESS- / ABSTURZ-MARKER

Abstürze oder Neustarts des Prozesses `sslvpnd` · Crash-Logs am SSL-VPN-Daemon

NACHLAGERUNG

neue oder unerwartete Administratorkonten, veränderte Konfiguration, unbekannte Skripte / ausgehende Verbindungen

Zur Einordnung: Fortinet und CISA nennen keine belastbare, geräteübergreifende Signaturliste. Die genannten Marker sind Anhaltspunkte aus öffentlicher Analyse und der beobachteten Ausnutzung – kein Ersatz für die forensische Prüfung Ihrer SSL-VPN-, System- und Crash-Logs. Erfahrene Angreifer entfernen Spuren.

Wichtig: Eine erfolgreiche Ausnutzung ermöglicht Codeausführung auf der Firewall selbst. Ein reiner Patch entfernt bereits untergeschobene Konten, Konfigurationsänderungen oder Persistenz nicht – ohne forensische Prüfung bleibt eine erfolgte Kompromittierung unsichtbar. Die Schwachstelle wird nachweislich auch in Ransomware-Kampagnen genutzt.

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: Anomalien am SSL-VPN-Dienst – Abstürze von sslvpnd, präparierte HTTP-Anfragen und neue Administratorkonten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte FortiOS-/FortiProxy-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

- SSL-VPN heute deaktivieren oder strikt abschotten, Patch innerhalb der CISA-Frist (16.02.2024) bzw. unverzüglich einspielen.
- Wegen aktiver Ausnutzung und Ransomware-Nutzung forensisch prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Grundsatz durchsetzen: Fernzugangs-Dienste nie ungeschützt exponieren, SSL-VPN nur mit MFA.

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-2024-21762 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-24-015 (CVE-2024-21762) · NVD (nvd.nist.gov, CVSS 3.1 Basiswert 9,8, CWE-787) · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 09.02.2024, Frist 16.02.2024, Ransomware-Nutzung bekannt). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.