AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2023-27997

Pre-Auth-RCE im Fortinet SSL-VPN („XORtigate“).

Ein nicht authentifizierter Angreifer aus dem Netz kann über einen Heap-basierten Pufferüberlauf in der SSL-VPN-Komponente von FortiOS und FortiProxy beliebigen Code auf der Firewall ausführen – ohne gültige Zugangsdaten und ohne Zutun eines Nutzers. Betroffen ist genau das Gerät, das das Unternehmensnetz nach außen absichern soll. Die unter dem Namen „XORtigate“ bekannte Schwachstelle wird aktiv ausgenutzt und steht im CISA-KEV-Katalog, auch im Zusammenhang mit Ransomware.

> **Geschäftsrisiko:** Vollständige Kompromittierung des Perimeter-Gateways: Der Angreifer erlangt Codeausführung auf der Firewall selbst, kann VPN-Sitzungen und Zugangsdaten abgreifen, sich ins interne Netz bewegen und Ransomware ausbringen. Ein solcher Vorfall hat unmittelbares Potenzial für Datenabfluss, Betriebsunterbrechung und eine meldepflichtige Sicherheitsverletzung nach NIS-2 / DSGVO.

9,8 / 10

KRITISCH
CVSS 3.1 BASISWERT

`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 Opfers – vollständige Übernahme des Firewall-Systems mit Codeausführung. Der NVD bewertet die Lücke mit 9,8; Fortinet selbst stuft sie im eigenen Advisory mit 9,2 ein. Beide liegen im Bereich KRITISCH.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Juni 2023	FortiOS 6.0 – 7.2 und FortiProxy 1.1 – 7.2 mit aktiviertem SSL-VPN	Sofort

Das Wichtigste in 60 Sekunden.

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

Pre-Auth RCE
Codeausführung ohne Anmeldung

Aktiv
ausgenutzt · CISA KEV (seit 13.06.2023)

CWE-122
Heap-based Buffer Overflow

Die Ursache: Die SSL-VPN-Komponente von FortiOS und FortiProxy verarbeitet speziell präparierte Anfragen fehlerhaft und schreibt dabei über die Grenzen eines Speicherbereichs auf dem Heap hinaus (**Heap-based Buffer Overflow**, CWE-122 / CWE-787). Ein **nicht authentifizierter** Angreifer kann diesen Überlauf gezielt ausnutzen, um eigenen Code einzuschleusen und auf dem Gerät auszuführen. Anfällig ist jedes System mit aktiviertem SSL-VPN-Webportal.

ANGRIFFSKETTE

01	02	03	04
SSL-VPN exponiert – das SSL-VPN-Webportal ist aus dem Internet erreichbar	**Präparierte Anfrage** – unauthentifizierte, gezielt gestaltete Anfrage löst den Heap-Überlauf aus	**Codeausführung** – der Angreifer führt beliebigen Code direkt auf der Firewall aus	**Ausweitung** – VPN-Zugänge und Sitzungen abgreifen, ins interne Netz bewegen, bis hin zur Ransomware

Betroffenheit & Fixversionen

FortiOS / FortiProxy-Version	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.2	7.2.0 – 7.2.4	7.2.5
FortiOS 7.0	7.0.0 – 7.0.11	7.0.12
FortiOS 6.4	6.4.0 – 6.4.12	6.4.13
FortiOS 6.2	6.2.0 – 6.2.13	6.2.14
FortiOS 6.0	6.0.0 – 6.0.16	6.0.17
FortiProxy 7.2	7.2.0 – 7.2.3	7.2.4
FortiProxy 7.0	7.0.0 – 7.0.9	7.0.10
FortiProxy 2.0	2.0.0 – 2.0.12	2.0.13
FortiProxy 1.1 / 1.2	alle Versionen	auf gepatchten Zweig migrieren

Betroffen sind FortiOS und FortiProxy in den genannten Versionen mit aktiviertem SSL-VPN. Fortinet nennt zusätzlich die FortiOS-6K7K-Plattformen mit eigenen Fixständen – prüfen Sie diese anhand des Hersteller-Advisories. Systeme **ohne** aktiviertes SSL-VPN sind für diese Schwachstelle nicht angreifbar; ein Update wird dennoch dringend empfohlen.

Regulatorischer Hinweis: Firewalls sind zentrale Sicherheitskomponenten – eine bestätigte Kompromittierung oder ein Abfluss von Zugangs- bzw. personenbezogenen 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 – SSL-VPN absichern, patchen, Zugangsdaten rotieren, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Patchen oder SSL-VPN deaktivieren	VPN-Zugangsdaten & Sitzungen rotieren	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Prüfen, ob FortiOS- oder FortiProxy-Geräte in einer betroffenen Version im Einsatz sind und ob das `SSL-VPN` aktiviert und aus dem Internet erreichbar ist. Version über die CLI (`get system status`) oder die Weboberfläche verifizieren.

02 Patchen (vorrangig)

Auf die jeweils gefixte Version aktualisieren: FortiOS `7.2.5` / `7.0.12` / `6.4.13` / `6.2.14` / `6.0.17` oder neuer, FortiProxy entsprechend `7.2.4` / `7.0.10` / `2.0.13`. Damit ist der Pufferüberlauf geschlossen.

03 Behelfsmaßnahme, wenn Patch nicht sofort möglich

Ist ein sofortiges Update nicht möglich, das `SSL-VPN` vollständig deaktivieren. Von Fortinet als einzige belastbare Behelfsmaßnahme benannt – eine reine Firewall-Regel auf dem betroffenen Gerät genügt nicht.

04 Zugangsdaten als kompromittiert behandeln

Bei exponierten, ungepatchten Geräten alle VPN-Benutzer- und Admin-Zugangsdaten sowie vorinstallierte Zertifikate/Schlüssel rotieren und aktive VPN-Sitzungen beenden – ein Patch macht bereits abgeflossene Geheimnisse nicht ungültig.

05 Kompromittierung ausschließen

System- und VPN-Logs auf ungewöhnliche Anmeldungen, unbekannte Administrator-Konten, geänderte Konfigurationen und auffällige Prozesse prüfen. Bei Verdacht die von Fortinet und CISA veröffentlichten Indikatoren abgleichen.

```
execute log filter category event ; execute log display
```

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE AKTIVITÄT

Unerwartete Abstürze/Neustarts des `sslvpnd`-Prozesses oder Crash-Logs

KOMPROMITTIERUNGS-CHECK

Neue oder unbekannte Admin-Konten, geänderte Firewall-/VPN-Konfiguration

FOLGEINDIKATOREN

Ungewöhnliche VPN-Anmeldungen und laterale Bewegung aus dem VPN-Netz

Zur Einordnung: Die Ausnutzung läuft über reguläre SSL-VPN-Anfragen und hinterlässt nicht zwingend eindeutige Spuren. Fortinet nennt Abstürze des SSL-VPN-Dienstes als möglichen Hinweis; der zuverlässigste Indikator bleibt die Auswertung Ihrer VPN- und Authentifizierungs-Logs sowie ein Abgleich mit den offiziellen IoCs von Fortinet und CISA.

Wichtig: Diese Schwachstelle trifft die Firewall selbst – das Gerät, das das Netz schützen soll. Weil sie unauthentifiziert und aus dem Internet ausnutzbar ist, aktiv ausgenutzt wird und im KEV-Katalog steht, zählt jede Stunde. Wer nicht sofort patchen kann, muss das SSL-VPN abschalten. Und da bereits abgeflossene Zugangsdaten einen Patch überdauern, ist deren Rotation 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: Anomale SSL-VPN-Anfragen, Abstürze des sslvpnd-Prozesses und verdächtige VPN-Anmeldungen auf Fortinet-Geräten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte 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 / FortiProxy-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

- Betroffene FortiOS-/FortiProxy-Geräte heute auf die gefixte Version patchen; wo das nicht sofort geht, das SSL-VPN abschalten.
- VPN- und Admin-Zugangsdaten der exponierten Geräte rotieren und aktive Sitzungen beenden lassen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung nach NIS-2 / DSGVO.

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-2023-27997 und dem FortiOS / FortiProxy-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-23-097 (veröffentlicht 12.06.2023, Fixversionen) · NVD CVE-2023-27997 (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-122; Fortinet-eigener Score 9,2) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 13.06.2023, Frist 04.07.2023, Nutzung u. a. in Ransomware) · Bishop Fox Attack Research („XORtigate“, PoC). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.