AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2018-13379

Pre-Auth Path Traversal im FortiOS SSL-VPN-Webportal.

Ein nicht authentifizierter Angreifer aus dem Netz kann über eine speziell präparierte HTTP-Anfrage an das SSL-VPN-Webportal beliebige FortiOS-Systemdateien auslesen. Besonders brisant: die Session-Datei sslvpn_websession enthält Benutzernamen und Passwörter aktiver VPN-Nutzer im Klartext. Mit diesen Zugangsdaten steht der Fernzugang ins Unternehmensnetz offen. Die Schwachstelle wird seit 2019 aktiv ausgenutzt und ist bis heute ein bevorzugtes Einfallstor für Ransomware- und Staatsakteure.

> **Geschäftsrisiko:** Diebstahl gültiger VPN-Zugangsdaten und in der Folge unbefugter Fernzugriff auf das interne Netz – 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 – über eine manipulierte HTTP-Anfrage lassen sich Systemdateien des SSL-VPN-Gateways herunterladen, darunter die Session-Datei mit Zugangsdaten im Klartext. Fortinet selbst bewertet die Lücke mit CVSS 3.1 zu 9,1.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
August 2019	FortiOS 5.4.6–5.4.12, 5.6.3–5.6.7, 6.0.0–6.0.4 (nur mit aktiviertem SSL-VPN-Webportal)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (3.1)

Pre-Auth
ohne Anmeldung auslesbar

Aktiv
ausgenutzt · CISA KEV (seit 03.11.2021)

CWE-22
Path Traversal

Die Ursache: Das SSL-VPN-Webportal von FortiOS prüft in den betroffenen Versionen den `lang`-Parameter der Sprachdatei-Anfrage nicht ausreichend. Über eingeschleuste Verzeichniswechsel (`../`) kann ein **nicht authentifizierter** Angreifer aus dem Verzeichnisbaum ausbrechen und beliebige Systemdateien herunterladen – insbesondere `/dev/cmdb/sslvpn_websession`, in der Zugangsdaten angemeldeter VPN-Nutzer im Klartext abgelegt sind.

ANGRIFFSKETTE

01 **SSL-VPN exponiert** – das FortiOS-Webportal ist über das Internet erreichbar

02 **Path-Traversal-Anfrage** – manipulierter `lang`-Parameter bricht aus dem Verzeichnis aus

03 **Session-Datei auslesen** – `sslvpn_websession` liefert Benutzernamen und Passwörter im Klartext

04 **Ausweitung** – Anmeldung am VPN mit gültigen Zugangsdaten, dann seitliche Bewegung ins interne Netz

Betroffenheit & Fixversionen

FortiOS-Version	Verwundbar bis	Fixversion (Ziel)
FortiOS 5.4	5.4.6 – 5.4.12	5.4.13
FortiOS 5.6	5.6.3 – 5.6.7	5.6.8
FortiOS 6.0	6.0.0 – 6.0.4	6.0.5 / 6.2.0
FortiProxy	1.0.0 – 1.2.8, 2.0.0	1.2.9 / 2.0.1

Betroffen sind ausschließlich Geräte mit **aktiviertem SSL-VPN-Webportal** in den genannten FortiOS- und FortiProxy-Versionen. FortiOS 6.2.0 und neuer sowie die genannten Patch-Stände sind nicht mehr anfällig. Reine IPsec-VPN-Konfigurationen ohne SSL-VPN-Webportal sind von dieser Lücke nicht betroffen.

Regulatorischer Hinweis: Ein bestätigter Abfluss von Zugangsdaten oder 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.

ZEITACHSE

24.05.2019
Fortinet veröffentlicht Advisory FG-IR-18-384 mit Fixes (5.4.13, 5.6.8, 6.0.5)

Aug. 2019
Öffentliche Exploit-Details (Black Hat / DEF CON); massenhaftes Scannen beginnt

Nov. 2020
Zugangsdaten von rund 50.000 verwundbaren VPN-Gateways werden im Netz veröffentlicht

03.11.2021
CISA nimmt CVE-2018-13379 in den KEV-Katalog auf – anhaltende aktive Ausnutzung

Ihr Maßnahmenplan.

In dieser Reihenfolge – Exposition prüfen, patchen, alle VPN-Zugangsdaten rotieren, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

Prüfen, ob ein FortiGate/FortiProxy mit aktiviertem SSL-VPN-Webportal in einer der betroffenen Versionen betrieben wird und aus dem Internet erreichbar ist. Auch länger nicht aktualisierte oder vergessene Geräte am Perimeter einbeziehen.

02 Sofort mitigieren (falls kein sofortiger Patch möglich)

SSL-VPN-Webportal vorübergehend deaktivieren oder den Zugriff strikt auf vertrauenswürdige Quell-IPs begrenzen. Von Fortinet als Behelfsmaßnahme benannt.

```
config vpn ssl settings unset source-interface end
```

03 Patchen

Auf einen bereinigten Stand aktualisieren: FortiOS `5.4.13`, `5.6.8`, `6.0.5` oder `6.2.0` und neuer (FortiProxy `1.2.9` / `2.0.1`). Damit ist der Path Traversal geschlossen.

04 Zugangsdaten als kompromittiert behandeln

Da die Session-Datei Zugangsdaten im Klartext enthielt, sämtliche VPN- und lokal auf dem Gerät hinterlegten Konten-Passwörter zurücksetzen – ein Patch macht bereits abgeflossene Zugangsdaten nicht ungültig. Zusätzlich Multi-Faktor-Authentifizierung für alle VPN-Nutzer aktivieren.

05 Kompromittierung ausschließen

SSL-VPN- und Web-Zugriffslogs auf Anfragen mit `/remote/fgt_lang` und `../`-Sequenzen sowie auf VPN-Anmeldungen aus untypischen Quell-IPs durchsuchen. Fehlende Logs für den relevanten Zeitraum sind selbst ein Warnsignal.

Kompromittierungs-Indikatoren (IoCs)

EXPLOIT-SIGNATUR

HTTP-Anfragen auf `/remote/fgt_lang?lang=/../../../..//////////dev/cmdb/sslvpn_websession`

AUFFÄLLIGE AKTIVITÄT

Zugriffe mit `../`-Verzeichniswechseln auf `/remote/fgt_lang` aus fremden Quellen

FOLGEINDIKATOREN

VPN-Anmeldungen mit gültigen Konten aus ungewöhnlichen Ländern/IPs; unbekannte lokale Admin-Konten

Zur Einordnung: Der zuverlässigste Nachweis ist die Auswertung der SSL-VPN- und Web-Zugriffslogs auf den Exploit-Pfad. Da die betroffenen Geräte teils seit 2019 exponiert waren, reicht das Fehlen von Treffern im aktuellen Log nicht als Entwarnung – historische Logs und eine mögliche frühere Kompromittierung sind mit zu bewerten.

Wichtig: Der Kern des Risikos liegt nicht im bloßen Dateizugriff, sondern in den ausgelesenen Klartext-Zugangsdaten: Sind VPN-Passwörter einmal abgeflossen, bleibt der Fernzugang auch nach dem Patch bestehen. Deshalb ist die Rotation aller Zugangsdaten und die Einführung von Multi-Faktor-Authentifizierung 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: Path-Traversal-Anfragen an /remote/fgt_lang und VPN-Anmeldungen mit darüber abgeflossenen Zugangsdaten 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-SSL-VPN-Gateways 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 prüfen und patchen oder das Webportal bis zum Patch abschalten.
- Alle VPN- und lokalen Geräte-Zugangsdaten rotieren lassen und Multi-Faktor-Authentifizierung erzwingen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – 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-2018-13379 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-18-384 (Fixes: FortiOS 5.4.13 / 5.6.8 / 6.0.5 / 6.2.0, FortiProxy 1.2.9 / 2.0.1) · NVD (NIST CVSS 3.1: 9,8 KRITISCH; Fortinet CVSS 3.1: 9,1; CWE-22) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 03.11.2021). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.