AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2018-13383

Heap-Buffer-Overflow im FortiOS SSL-VPN-Web-Portal.

Im Reverse-Proxy-Modus des FortiOS SSL-VPN-Web-Portals werden JavaScript-href-Daten beim Weiterleiten von Webseiten fehlerhaft verarbeitet. Öffnet ein bereits angemeldeter SSL-VPN-Nutzer eine entsprechend präparierte Webseite, kommt es zu einem Heap-Buffer-Overflow – der SSL-VPN-Web-Dienst stürzt ab und trennt die angemeldeten Nutzer. Fortinet schließt eine darüber hinausgehende Codeausführung nicht aus. Die Schwachstelle wird von staatsnahen Angreifern aktiv ausgenutzt und steht seit Januar 2022 im CISA-KEV-Katalog.

> **Geschäftsrisiko:** Ausfall des SSL-VPN-Fernzugangs (Denial of Service) für alle angemeldeten Nutzer und – im ungünstigen Fall – Codeausführung auf dem Gateway. Da das Gerät der zentrale Fernzugangs-Knoten ist, drohen Betriebsunterbrechung, Verlust des sicheren Remote-Zugriffs und, bei erfolgreicher Kompromittierung, ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO.

6,5 / 10

MITTEL
CVSS 3.1 BASISWERT

Niedrig | **Mittel** | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H` – aus dem Netz und ohne besondere Rechte, aber erst wenn ein angemeldeter Nutzer eine manipulierte, über das Portal weitergeleitete Webseite öffnet – dann bricht der SSL-VPN-Web-Dienst ab (Denial of Service), mit Potenzial für Codeausführung. Fortinet selbst bewertet die Lücke mit 4,3.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
April 2021	FortiOS 6.0.0–6.0.4 · 5.6.0–5.6.10 · 5.4.0–5.4.12 · ≤ 5.2.14 FortiProxy 2.0.0 · ≤ 1.2.8	Hoch

Das Wichtigste in 60 Sekunden.

6,5 · MITTEL
CVSS-Schweregrad (3.1, NVD)

Auth + UI
angemeldeter Nutzer muss Seite öffnen

Aktiv
ausgenutzt · CISA KEV (seit 10.01.2022)

CWE-787
Out-of-bounds Write (Heap-Overflow)

Die Ursache: Das SSL-VPN-Web-Portal von FortiOS arbeitet als Reverse-Proxy und leitet externe Webseiten an den angemeldeten Nutzer weiter. Beim Verarbeiten von JavaScript-href-Daten in solchen weitergeleiteten Seiten prüft FortiOS die Datenlänge nicht ausreichend und schreibt über den zugewiesenen Speicherbereich hinaus (CWE-787, Heap-Buffer-Overflow). Das führt zum Abbruch des SSL-VPN-Web-Dienstes; eine weitergehende Codeausführung schließt der Hersteller nicht aus. Der reine Tunnel-Modus des SSL-VPN ist nicht betroffen.

ANGRIFFSKETTE

01 **SSL-VPN-Web-Portal erreichbar** – FortiGate mit aktivem SSL-VPN im Web-/Reverse-Proxy-Modus

02 **Nutzer angemeldet** – ein authentifizierter SSL-VPN-Nutzer verwendet das Web-Portal

03 **Manipulierte Seite öffnen** – der Nutzer ruft eine präparierte, über das Portal weitergeleitete Webseite mit fehlerhaften JavaScript-href-Daten auf

04 **Heap-Overflow** – Absturz des SSL-VPN-Web-Dienstes (DoS), potenziell Codeausführung auf dem Gateway

Betroffenheit & Fixversionen

FortiOS-Version	Verwundbar bis	Fixversion (Ziel)
FortiOS 6.0.x	6.0.0 – 6.0.4	6.0.5
FortiOS 5.6.x	5.6.0 – 5.6.10	5.6.11
FortiOS 5.4.x	5.4.0 – 5.4.12	5.4.13
FortiOS 5.2.x	≤ 5.2.14	5.2.15
FortiProxy	2.0.0 · ≤ 1.2.8	siehe FG-IR-20-229

Betroffen ist ausschließlich der **Web-/Reverse-Proxy-Modus** des SSL-VPN. Wer FortiOS auf 5.2.15, 5.4.13, 5.6.11, 6.0.5 oder 6.2.0 und neuer betreibt, ist gegen diese Lücke geschützt. Der reine SSL-VPN-Tunnel-Modus ist nicht anfällig. FortiProxy wird gesondert im Advisory FG-IR-20-229 behandelt.

Regulatorischer Hinweis: Führt die Ausnutzung zu einer erheblichen Störung des Fernzugangs oder zu einer bestätigten Kompromittierung, kann eine Meldepflicht bestehen – DSGVO unverzüglich (i. d. R. 72 h) bei Betroffenheit personenbezogener Daten, NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

26.11.2019
Fortinet veröffentlicht Advisory FG-IR-18-388 samt Fix-Versionen

02.04.2021
FBI und CISA warnen (AA21-092A) vor aktiver Ausnutzung

10.01.2022
CISA nimmt CVE-2018-13383 in den KEV-Katalog auf – aktive Ausnutzung

24.01.2022
KEV-Frist für US-Behörden zum Patchen/Mitigieren

Ihr Maßnahmenplan.

In dieser Reihenfolge – erreichbare Instanzen finden, mitigieren, patchen, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Betroffene FortiGate identifizieren / mitigieren	Auf gefixte FortiOS-Version patchen	Threat Hunting / Log-Auswertung

01 Betroffenheit feststellen

Prüfen, ob FortiGate-Geräte mit FortiOS unterhalb der Fix-Versionen (`5.2.15` / `5.4.13` / `5.6.11` / `6.0.5`) im Einsatz sind und ob das SSL-VPN im Web-/Reverse-Proxy-Modus aktiviert ist.

02 Sofort mitigieren (vor dem Patch)

Als Behelfsmaßnahme das SSL-VPN ausschließlich im Tunnel-Modus betreiben, den Web-Portal-Zugriff auf vertrauenswürdige HTTP-Server begrenzen oder das SSL-VPN vorübergehend per CLI deaktivieren.

03 Patchen

FortiOS auf `5.2.15`, `5.4.13`, `5.6.11`, `6.0.5`, `6.2.0` oder neuer aktualisieren. Damit ist der Heap-Buffer-Overflow geschlossen.

04 Kompromittierung ausschließen

Da dieselben FortiOS-SSL-VPN-Lücken (u. a. CVE-2018-13379) für den Diebstahl von Zugangsdaten genutzt wurden, alle SSL-VPN-Zugangsdaten prüfen und rotieren sowie Logs auf unautorisierte Anmeldungen und Dienstabstürze durchsehen.

05 Fernzugang härten

Multi-Faktor-Authentifizierung für den SSL-VPN-Zugang durchsetzen, Zugriff auf notwendige Quell-IP-Bereiche begrenzen und ein regelmäßiges FortiOS-Patch-Regime etablieren.

```
config vpn ssl settings\n set source-address <trusted-range>\nend
```

Kompromittierungs-Indikatoren (IoCs)

DIENST-ABSTURZ

Wiederholte Abbrüche des SSL-VPN-Web-Dienstes
und Trennung angemeldeter Nutzer

AUFFÄLLIGE AKTIVITÄT

Aufruf ungewöhnlicher, über das Portal weitergeleiteter Webseiten mit fehlerhaftem JavaScript-href

FOLGEINDIKATOREN

Fremd-/Neuanmeldungen am SSL-VPN mit
bekannten Nutzerkonten aus fremden Quell-IPs

Zur Einordnung: Ein Crash des SSL-VPN-Web-Dienstes ist der unmittelbarste Hinweis. Da die eigentliche Auslösung über eine reguläre, weitergeleitete Web-Anfrage erfolgt, ist sie ohne detaillierte Zugriffs- und Krash-Logs schwer eindeutig zuzuordnen – die zuverlässigste Grundlage ist die Auswertung Ihrer SSL-VPN- und Authentifizierungs-Logs.

Wichtig: Diese Schwachstelle gehört zu der Gruppe von FortiOS-SSL-VPN-Lücken, die staatsnahe Angreifer seit 2021 aktiv ausnutzen. Auch wenn der Fix seit 2019 vorliegt, bleiben ungepatchte, aus dem Internet erreichbare FortiGate-Geräte ein bevorzugtes Ziel. Entscheidend ist, nicht nur zu patchen, sondern zuvor abgeflossene SSL-VPN-Zugangsdaten als kompromittiert zu behandeln und zu rotieren.

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: Wiederholte SSL-VPN-Web-Dienst-Abstürze und anomale Anmeldungen an FortiGate-SSL-VPN-Zugängen fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte FortiGate-SSL-VPN-Web-Portale 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

- Erreichbare FortiGate mit SSL-VPN-Web-Portal identifizieren und heute mitigieren (Tunnel-Modus / Zugriffsbeschränkung); Patch unverzüglich einplanen.
- SSL-VPN-Zugangsdaten prüfen und rotieren lassen – die zugehörigen FortiOS-Lücken wurden für Credential-Diebstahl genutzt.
- Prüfen lassen, ob bereits Ausnutzung oder unautorisierter 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-2018-13383 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-18-388 · NVD (CVSS 3.1: 6,5 MITTEL, Vektor AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H; CWE-787; Fortinet-CNA-Score 4,3) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 10.01.2022) · FBI/CISA Joint Advisory AA21-092A. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.