AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2018-13382

Unautorisierte Passwortänderung im Fortinet SSL-VPN-Portal („magic").

Im SSL-VPN-Web-Portal von FortiOS und FortiProxy steckt ein Autorisierungsfehler: Ein nicht authentifizierter Angreifer kann aus dem Netz über speziell präparierte HTTP-Anfragen das Passwort eines lokal authentifizierten SSL-VPN-Portal-Nutzers neu setzen und sich damit dessen Konto aneignen. Ist keine Zwei-Faktor-Authentifizierung aktiv, steht anschließend der VPN-Zugang ins interne Netz offen. Die Schwachstelle – im Fortinet-Code über einen fest hinterlegten „magic"-Wert erreichbar – wird seit Jahren aktiv ausgenutzt und steht im CISA-KEV-Katalog.

Geschäftsrisiko: Übernahme von SSL-VPN-Konten und darüber unbefugter Zugang zum internen Netz – mit Potenzial für Datenabfluss, laterale Ausbreitung, Ransomware und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

7,5 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N` – aus dem Netz, ohne Anmeldung, ohne Zutun – ein Angreifer kann über präparierte HTTP-Anfragen das Passwort eines lokal authentifizierten SSL-VPN-Portal-Nutzers ändern und dessen Konto übernehmen. Fortinet bewertet die Lücke im eigenen Advisory (FG-IR-18-389) mit 8,9.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
spätestens seit 2020 (Massenausnutzung, Credential-Leaks)	FortiOS 5.4.1-5.4.10, 5.6.0-5.6.8, 6.0.0-6.0.4 FortiProxy 1.0.0-1.0.7, 1.1.0-1.1.6, 1.2.0-1.2.8, 2.0.0 nur mit aktiviertem SSL-VPN und lokaler Authentifizierung	Sofort

Das Wichtigste in 60 Sekunden.

7,5 · HOCH
CVSS-Schweregrad (3.1)

Unauth
ohne Anmeldung – Passwort änderbar

Aktiv
ausgenutzt · CISA KEV (seit 10.01.2022)

CWE-863
Fehlerhafte Autorisierung

Die Ursache: Das SSL-VPN-Web-Portal prüft in den betroffenen Versionen die Berechtigung für den Passwort-Änderungsvorgang nicht korrekt. Fortinet hatte auf Kundenwunsch einen fest im Code hinterlegten „magic"-Wert eingebaut, mit dem sich ein ablaufendes Portal-Passwort erneuern lässt. Ein **nicht authentifizierter** Angreifer kann diesen Ablauf über eine präparierte HTTP-Anfrage anstoßen und so das Passwort eines **lokal authentifizierten** SSL-VPN-Portal-Nutzers überschreiben – ganz ohne gültige Zugangsdaten.

ANGRIFFSKETTE

01 **SSL-VPN erreichbar** – das Web-Portal ist aus dem Internet erreichbar und nutzt lokale Authentifizierung

02 **„magic"-Anfrage** – speziell präparierte HTTP-Anfrage an den Passwort-Änderungs-Endpunkt, ohne Anmeldung

03 **Passwort überschreiben** – das Passwort eines lokalen SSL-VPN-Portal-Nutzers wird neu gesetzt

04 **Kontoübernahme** – mit dem neuen Passwort per VPN ins interne Netz; ohne 2FA freier Zugang

Betroffenheit & Fixversionen

FortiOS-Version	Verwundbar bis	Fixversion (Ziel)
FortiOS 5.4.x	`5.4.1-5.4.10`	`5.4.11`
FortiOS 5.6.x	`5.6.0-5.6.8`	`5.6.9`
FortiOS 6.0.x	`6.0.0-6.0.4`	`6.0.5`
FortiOS 6.2 · 5.4.0 und älter · Branch 5.2	nicht betroffen	—
FortiProxy	`1.0.0-1.0.7, 1.1.0-1.1.6, 1.2.0-1.2.8, 2.0.0`	fehlerbereinigte FortiProxy-Version lt. Fortinet

Betroffen sind ausschließlich Systeme mit **aktiviertem SSL-VPN und lokaler Authentifizierung**. FortiOS `6.2.0` und höher, `5.4.0` und älter sowie der Branch `5.2` sind nicht betroffen. FortiProxy ist laut NVD in den genannten Versionen ebenfalls anfällig – hier auf eine von Fortinet als fehlerbereinigt ausgewiesene Version aktualisieren.

Regulatorischer Hinweis: Wird ein SSL-VPN-Konto übernommen und daraus ein Zugriff auf personenbezogene oder schützenswerte Daten möglich, kann eine meldepflichtige Verletzung vorliegen – 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

30.08.2019
Fortinet veröffentlicht Advisory FG-IR-18-389; Fixes in 5.4.11,

Nov. 2020
Zugangsdaten tausender FortiGate-SSL-VPNs kursieren

02.04.2021
Gemeinsames FBI/CISA-Advisory zur aktiven

10.01.2022
CISA nimmt CVE-2018-13382 in den KEV-Katalog auf (Frist für

Ihr Maßnahmenplan.

In dieser Reihenfolge – Zugriff härten, patchen, Portal-Passwörter zurücksetzen, Kompromittierung ausschließen.

01 Betroffenheit feststellen

Prüfen, ob FortiOS in einer Version unterhalb der Fixstände (`5.4.11` / `5.6.9` / `6.0.5`) läuft und ob das SSL-VPN-Web-Portal mit lokaler Authentifizierung aus dem Netz erreichbar ist. Nur diese Konstellation ist angreifbar.

02 Sofort mitigieren (vor dem Patch)

Von Fortinet benannte Behelfsmaßnahmen umsetzen: für alle lokalen SSL-VPN-Nutzer **Zwei-Faktor-Authentifizierung** erzwingen, die Authentifizierung auf LDAP/RADIUS umstellen oder – wenn nicht benötigt – das SSL-VPN-Web-Portal per CLI deaktivieren.

```
config vpn ssl settings unset source-interface unset source-address unset default-portal end
```

03 Patchen

Auf `FortiOS 5.4.11`, `5.6.9`, `6.0.5` bzw. `6.2.0` oder neuer aktualisieren (FortiProxy entsprechend). Damit ist der Autorisierungsfehler geschlossen.

04 Portal-Passwörter als kompromittiert behandeln

Da ein Angreifer Passwörter unbemerkt überschrieben haben kann, die Passwörter aller lokal authentifizierten SSL-VPN-Portal-Nutzer zurücksetzen und – wo möglich – dauerhaft 2FA aktivieren. Ein Patch macht bereits geänderte Passwörter nicht rückgängig.

05 Kompromittierung ausschließen

Ereignis- und VPN-Logs auf unautorisierte Passwortänderungen und auf ungewöhnliche SSL-VPN-Anmeldungen (fremde Quell-IPs, untypische Zeiten, neue Standorte) lokaler Konten durchsuchen.

```
execute log filter category 1 execute log display
```

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE AKTIVITÄT

Unautorisierte Passwortänderungen an lokalen SSL-VPN-Portal-Konten in den Event-Logs

ANOMALE ANMELDUNGEN

SSL-VPN-Logins aus fremden Quell-IPs, zu untypischen Zeiten oder von neuen Standorten

FOLGEINDIKATOREN

Laterale Bewegung ausgehend vom VPN-Segment, neue/unbekannte interne Sitzungen

Zur Einordnung: Der Angriff läuft über reguläre HTTP-Anfragen an das SSL-VPN-Portal und ist ohne detaillierte Zugriffs- und Authentifizierungs-Logs schwer nachzuweisen. Der zuverlässigste Indikator ist die Auswertung Ihrer FortiOS-Event- und VPN-Logs auf unerklärte Passwortänderungen und Fremdanmeldungen. Fehlende Auffälligkeiten schließen eine zurückliegende Ausnutzung nicht sicher aus.

Wichtig: Der Kern des Risikos ist die Kontoübernahme: Ein Angreifer setzt das Passwort zurück und meldet sich anschließend regulär am VPN an. Zwei-Faktor-Authentifizierung ist die wirksamste Absicherung – selbst mit einem neu gesetzten Passwort scheitert der Login ohne zweiten Faktor. Deshalb sind das Zurücksetzen aller Portal-Passwörter und die dauerhafte 2FA-Pflicht 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: Unautorisierte Passwortänderungen und anschließende SSL-VPN-Anmeldungen lokaler Konten 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-Portale mit lokaler Authentifizierung 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

- SSL-VPN heute härten: 2FA für alle lokalen Konten erzwingen oder das Portal abschalten; Patch auf einen festen FortiOS-Stand unverzüglich einplanen.
- Passwörter aller lokal authentifizierten SSL-VPN-Portal-Nutzer zurücksetzen lassen.
- 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-2018-13382 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-18-389 (CVSSv3 8,9 / High; Fixes 5.4.11, 5.6.9, 6.0.5, 6.2.0+) · NVD CVE-2018-13382 (CVSS 3.1: 7,5 / HOCH, Vektor AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N, CWE-863) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 10.01.2022, Frist 10.07.2022) · FBI/CISA Joint Advisory (02.04.2021).

Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.
Stand: 14.07.2026 · Argos Security · Cyber Defense Center