AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2020-12812

Umgehung der Zwei-Faktor-Authentifizierung im FortiOS SSL-VPN.

Ein Angreifer kann sich am FortiOS SSL-VPN anmelden, ohne nach dem zweiten Faktor (FortiToken) gefragt zu werden – indem er die Groß-/Kleinschreibung eines gültigen Benutzernamens verändert. Ursache ist eine unterschiedliche Behandlung der Schreibweise zwischen FortiGate und angebundenem LDAP-Verzeichnis. Mit gültigem Passwort, aber ohne zweiten Faktor, steht damit der VPN-Zugang und das dahinterliegende Unternehmensnetz offen. Die Schwachstelle steht seit November 2021 im CISA-KEV-Katalog und wird bis Ende 2025 aktiv ausgenutzt.

> **Geschäftsrisiko:** Unbefugter VPN-Zugang trotz aktivierter Zwei-Faktor-Authentifizierung – mit direktem Weg ins interne Netz, Potenzial für Datenabfluss, Ransomware-Vorbereitung und Betriebsunterbrechung sowie einem 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 – vollständige Anmeldung am SSL-VPN unter Umgehung des zweiten Faktors, mit anschließendem Vollzugriff auf das dahinterliegende Netz. Fortinet selbst bewertet die Lücke in seinem Advisory mit 5,2 (mittel); der maßgebliche NVD-Basiswert nach CVSS 3.1 liegt bei 9,8.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
3. November 2021	FortiOS 6.4.0 · 6.2.0–6.2.3 · 6.0.9 und älter	Sofort

Das Wichtigste in 60 Sekunden.

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

2FA-Bypass
zweiter Faktor wird umgangen

Aktiv
ausgenutzt · CISA KEV (seit 03.11.2021)

CWE-178
Improper Handling of Case Sensitivity

Die Ursache: FortiGate behandelt Benutzernamen standardmäßig als **groß-/kleinschreibungssensitiv**, die meisten LDAP-Verzeichnisse dagegen nicht. Meldet sich ein Nutzer mit einer abweichend geschriebenen Variante seines gültigen Namens an (etwa `Admin` statt `admin`), authentifiziert das LDAP-Verzeichnis ihn korrekt, FortiOS ordnet die Anmeldung aber keinem lokalen Konto mit hinterlegtem **zweiten Faktor** zu – und lässt ihn ohne FortiToken-Abfrage passieren.

ANGRIFFSKETTE

01 **SSL-VPN exponiert** – das FortiGate-VPN-Portal ist über das Internet erreichbar, 2FA per FortiToken ist aktiv

02 **Gültige Kennung** – der Angreifer kennt Benutzername und Passwort (z. B. aus Phishing, Leak oder Wiederverwendung)

03 **Schreibweise ändern** – Anmeldung mit veränderter Groß-/Kleinschreibung des Benutzernamens

04 **2FA umgangen** – Login gelingt ohne FortiToken-Abfrage; der Angreifer steht im internen Netz

Betroffenheit & Fixversionen

FortiOS-Version	Verwundbar bis	Fixversion (Ziel)
FortiOS 6.4	`6.4.0`	`6.4.1`
FortiOS 6.2	`6.2.0 – 6.2.3`	`6.2.4`
FortiOS 6.0	`6.0.9 und älter`	`6.0.10`

Betroffen ist der SSL-VPN-Dienst in FortiOS `6.4.0`, `6.2.0` bis `6.2.3` sowie `6.0.9` und älter, wenn die Benutzerauthentifizierung gegen ein LDAP-Verzeichnis läuft. Die Schwachstelle greift nur, wenn Zwei-Faktor-Authentifizierung eingesetzt wird – gerade die vermeintlich abgesicherten Zugänge sind gefährdet.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf das Unternehmensnetz oder ein Abfluss personenbezogener 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

24.07.2020
Fortinet veröffentlicht Advisory FG-IR-19-283, Fixes in 6.4.1 / 6.2.4 / 6.0.10; NVD publiziert CVE-2020-12812

03.11.2021
CISA nimmt CVE-2020-12812 in den KEV-Katalog auf – bestätigte aktive Ausnutzung

03.05.2022
KEV-Frist für US-Behörden zum Patchen

Dez. 2025
Fortinet warnt vor erneuter aktiver Ausnutzung; über 10.000 exponierte FortiGate-Firewalls betroffen

Ihr Maßnahmenplan.

In dieser Reihenfolge – exponierte Version feststellen, mitigieren, patchen, kompromittierte Zugänge ausschließen.

01 Betroffenheit feststellen

Prüfen, ob FortiOS in Version `6.4.0`, `6.2.0`–`6.2.3` oder `6.0.9` und älter im Einsatz ist, das SSL-VPN über das Internet erreichbar ist und die Benutzer gegen LDAP mit Zwei-Faktor-Authentifizierung anmelden.

02 Sofort mitigieren (vor dem Patch)

Als von Fortinet benannte Behelfsmaßnahme die Groß-/Kleinschreibungs-Prüfung erzwingen, damit abweichende Schreibweisen nicht mehr am zweiten Faktor vorbeikommen.

```
config user ldap edit <server> set username-case-sensitivity enable next end
```

03 Patchen

Auf `FortiOS 6.4.1`, `6.2.4`, `6.0.10` oder neuer aktualisieren. Damit ist der 2FA-Bypass geschlossen.

04 Zugänge als potenziell kompromittiert behandeln

Da ein Bypass unbemerkt erfolgt sein kann, VPN-Zugangsdaten der betroffenen Nutzer zurücksetzen und aktive VPN-Sessions terminieren. Ein Patch macht bereits erlangte Zugänge nicht ungültig.

05 Kompromittierung ausschließen

SSL-VPN-Authentifizierungs-Logs auf erfolgreiche Anmeldungen mit abweichender Groß-/Kleinschreibung des Benutzernamens und auf ungewöhnliche Quell-IP-Adressen oder Login-Zeiten durchsuchen.

```
# FortiOS: VPN-Login-Ereignisse auswerten execute log filter category event
execute log filter field subtype vpn execute log display
```

Kompromittierungs-Indikatoren (IoCs)

CHARAKTERISTISCHES MUSTER

Erfolgreiche SSL-VPN-Anmeldung mit abweichender Schreibweise eines gültigen Namens

`z. B. Admin statt admin`

AUFFÄLLIGE AKTIVITÄT

VPN-Logins ohne vorangehende FortiToken-/2FA-Ereignisse in den Logs

FOLGEINDIKATOREN

VPN-Anmeldungen aus fremden Ländern, zu ungewöhnlichen Zeiten oder von neuen Quell-IPs

Zur Einordnung: Ein sauberer Bypass hinterlässt eine erfolgreiche Anmeldung ohne 2FA-Abfrage – ohne detaillierte VPN-Authentifizierungs-Logs schwer zu erkennen. Der zuverlässigste Indikator ist der Abgleich erfolgreicher SSL-VPN-Logins gegen die Schreibweise der hinterlegten Konten und gegen Quell-IP/Geolokation.

Wichtig: Der zweite Faktor schützt hier nicht: Wer Benutzername und Passwort besitzt, umgeht die 2FA allein durch geänderte Schreibweise. Deshalb reicht es nicht, sich auf aktiviertes FortiToken zu verlassen – erst der Patch oder die erzwungene Case-Sensitivity schließt die Lücke, und bereits erlangte Zugänge müssen aktiv ausgeschlossen werden.

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: SSL-VPN-Anmeldungen mit abweichender Schreibweise des Benutzernamens und Logins ohne zugehöriges 2FA-Ereignis fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden über das Internet erreichbare, ungepatchte FortiOS-SSL-VPN-Portale mit LDAP-2FA 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

- Betroffene FortiGate-SSL-VPNs heute mitigieren (username-case-sensitivity enable) und Patch auf 6.4.1 / 6.2.4 / 6.0.10 unverzüglich einplanen.
- VPN-Zugangsdaten der betroffenen Nutzer zurücksetzen lassen und aktive Sessions terminieren.
- Prüfen lassen, ob bereits ein 2FA-Bypass 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-2020-12812 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-19-283 (Fixes FortiOS 6.4.1 / 6.2.4 / 6.0.10, Workaround username-case-sensitivity) · NVD (CVSS 3.1: 9,8 KRITISCH, Vektor AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H; CWE-178 / CWE-287) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 03.11.2021, Frist 03.05.2022). Fortinet selbst bewertet die Lücke im Advisory mit 5,2 (mittel); der hier ausgewiesene KRITISCH-Wert folgt dem maßgeblichen NVD-Basiswert. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.