AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2022-40684

Unauthentifizierter Admin-Zugriff über Authentication-Bypass in Fortinet FortiOS.

Ein nicht authentifizierter Angreifer aus dem Netz kann über speziell gestaltete HTTP- oder HTTPS-Anfragen die Authentifizierung der administrativen Verwaltungsschnittstelle umgehen und Verwaltungsoperationen mit vollen Rechten ausführen – etwa Admin-Konten anlegen, SSH-Schlüssel hinterlegen oder Konfigurationen ändern. Betroffen sind FortiOS, FortiProxy und der FortiSwitchManager. Die Schwachstelle wird seit Oktober 2022 aktiv ausgenutzt, ein öffentlicher Proof-of-Concept ist verfügbar.

> **Geschäftsrisiko:** Vollständige Übernahme der Firewall- und Proxy-Verwaltung durch Unbefugte – mit Potenzial für dauerhafte Hintertüren, Umgehung der Perimeter-Sicherheit, Datenabfluss, 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 – vollständige Übernahme der administrativen Verwaltungsschnittstelle. Fortinet bewertet die Lücke im eigenen Advisory mit 9,6.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Oktober 2022	FortiOS 7.0.0–7.0.6 / 7.2.0–7.2.1 FortiProxy 7.0.0–7.0.6 / 7.2.0 FortiSwitchManager 7.0.0 / 7.2.0	Sofort

Das Wichtigste in 60 Sekunden.

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

Auth-Bypass
ohne Anmeldung, volle Admin-Rechte

Aktiv
ausgenutzt · CISA KEV (seit 11.10.2022)

CWE-287
Improper Authentication

Die Ursache: In den betroffenen Versionen lässt sich die Authentifizierung der administrativen Verwaltungsschnittstelle über einen alternativen Pfad umgehen: Speziell gestaltete HTTP-/HTTPS-Anfragen – etwa mit gesetztem `Forwarded`-Header und dem internen Client `Node.js` als User-Agent – werden vom Gerät als vertrauenswürdige interne Anfragen behandelt. Ein **nicht authentifizierter** Angreifer kann dadurch privilegierte Verwaltungs-API-Aufrufe ausführen, ohne gültige Zugangsdaten zu besitzen.

ANGRIFFSKETTE

01
Verwaltungsschnittstelle exponiert – die HTTP-/HTTPS-Admin-Oberfläche ist über das Netz erreichbar

02
Anfrage fälschen – manipulierte, unauthentifizierte Anfrage mit gefälschtem Forwarded-Header täuscht eine interne Quelle vor

03
Als Admin agieren – privilegierte API-Aufrufe werden ausgeführt, als kämen sie von einem angemeldeten Administrator

04
Persistenz – Anlegen fremder Admin-Konten, Hinterlegen von SSH-Schlüsseln, Ändern der Konfiguration zur dauerhaften Übernahme

Betroffenheit & Fixversionen

Produkt / Version	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.2.x	`7.2.0 – 7.2.1`	`7.2.2`
FortiOS 7.0.x	`7.0.0 – 7.0.6`	`7.0.7`
FortiProxy 7.2.x	`7.2.0`	`7.2.1`
FortiProxy 7.0.x	`7.0.0 – 7.0.6`	`7.0.7`
FortiSwitchManager 7.2.x	`7.2.0`	`7.2.1`
FortiSwitchManager 7.0.x	`7.0.0`	`7.0.1`

Ältere Zweige (FortiOS 6.4 und 6.2, FortiProxy 2.0 / 1.x) sind laut Fortinet nicht betroffen. Für FG6000F- sowie 7000E/F-Modelle nennt Fortinet `FortiOS 7.0.5 B8001` oder neuer als korrigierten Stand. Maßgeblich ist die Erreichbarkeit der administrativen HTTP-/HTTPS-Schnittstelle über nicht vertrauenswürdige Netze.

Regulatorischer Hinweis: Firewalls und Proxies sind zentrale Sicherheitskomponenten – ein bestätigter unbefugter administrativer Zugriff oder ein daraus folgender Datenabfluss 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 – Verwaltungsschnittstelle abschotten, patchen, Konfiguration und Konten auf Manipulation prüfen.

SOFORT	KURZFRISTIG	PARALLEL
Admin-Schnittstelle abschotten / patchen	Admin-Konten & Schlüssel prüfen/rotieren	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Prüfen, ob FortiOS, FortiProxy oder FortiSwitchManager in einer der betroffenen Versionen im Einsatz ist und ob die administrative HTTP-/HTTPS-Schnittstelle aus nicht vertrauenswürdigen Netzen erreichbar ist.

02 Sofort mitigieren (vor dem Patch)

Wenn ein sofortiges Update nicht möglich ist: den HTTP-/HTTPS-Zugang zur Verwaltungsschnittstelle deaktivieren oder den Zugriff per `local-in policy` / Trusted-Hosts strikt auf autorisierte IP-Adressen begrenzen. Von Fortinet als Behelfsmaßnahme benannt.

03 Patchen

Auf einen korrigierten Stand aktualisieren: FortiOS `7.0.7` bzw. `7.2.2`, FortiProxy `7.0.7` bzw. `7.2.1`, FortiSwitchManager `7.0.1` bzw. `7.2.1` oder neuer.

04 Kompromittierung ausschließen

Konfiguration auf unbekannte Administrator-Konten, fremde SSH-Schlüssel, geänderte Admin-Profile und neue local-in-Policies prüfen. Die von Fortinet genannten Indikatoren im Log abgleichen.

05 Zugangsdaten & Schlüssel behandeln

Falls Anzeichen für einen Zugriff bestehen, alle Administrator-Passwörter zurücksetzen, hinterlegte SSH-Schlüssel prüfen/erneuern und die Gerätekonfiguration gegen einen bekannt-guten Stand abgleichen – ein Patch entfernt bereits angelegte Hintertüren nicht.

Kompromittierungs-Indikatoren (IoCs)

LOG-INDIKATOR

Verwaltungsaktionen mit `user=Local_Process_Access` im Log

FREMDES ADMIN-KONTO

Neu angelegter Super-Admin `fortigate-tech-support`

PERSISTENZ

Unbekannte SSH-Schlüssel oder fremde local-in-Policies in der Konfiguration

Zur Einordnung: Der Log-Eintrag user=Local_Process_Access in Verbindung mit Verwaltungsaktionen und das Konto fortigate-tech-support sind die von Fortinet genannten konkreten Kompromittierungshinweise. Da die Ausnutzung über reguläre HTTP-/HTTPS-Anfragen erfolgt, ist ohne detaillierte Zugriffs-Logs eine saubere Auswertung der Verwaltungs- und Authentifizierungsereignisse der zuverlässigste Indikator.

Wichtig: Der Kern des Risikos ist die Persistenz: Hat ein Angreifer die Verwaltung einmal übernommen und ein Admin-Konto, einen SSH-Schlüssel oder eine Policy hinterlegt, bleibt der Zugang auch nach dem Patch bestehen. Deshalb ist die Prüfung der Konfiguration auf Manipulation 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: Unauthentifizierte Verwaltungsanfragen an die Fortinet-Admin-Schnittstelle und das Auftauchen fremder Admin-Konten oder Log-Einträge mit Local_Process_Access 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-/FortiSwitchManager-Verwaltungsschnittstellen 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

- Administrative HTTP-/HTTPS-Schnittstelle der Fortinet-Geräte heute aus dem Internet nehmen oder strikt per IP-Allowlist begrenzen; Patch unverzüglich einplanen.
- Konfiguration jedes betroffenen Geräts auf fremde Admin-Konten, SSH-Schlüssel und Policies prüfen 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-2022-40684 und dem FortiOS-Perimeter.

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

Termin buchen

[illegible] / AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H, CWE-287; Fortinet-eigene Bewertung 9,6 / CWE-288) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 11.10.2022, Frist 01.11.2022) · Horizon3.ai Attack Research (öffentlicher PoC, 13.10.2022). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.