AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2021-44168

Datei-Download ohne Integritätsprüfung in Fortinet FortiOS.

In den betroffenen FortiOS-Versionen lädt der CLI-Befehl execute restore src-vis Update-Pakete, ohne deren Integrität oder Signatur zu prüfen. Ein lokal authentifizierter Angreifer kann darüber ein manipuliertes Paket unterschieben und beliebige Dateien und Programmcode auf die Firewall schreiben – die ideale Grundlage für einen dauerhaften, schwer auffindbaren Implantat auf dem Perimeter-Gerät. Fortinet hat einen Fall bestätigt, in dem die Schwachstelle bereits missbraucht wurde; die CISA führt sie im Katalog aktiv ausgenutzter Schwachstellen.

> **Geschäftsrisiko:** Ein Angreifer mit Admin-Zugang – etwa über gestohlene Zugangsdaten oder eine vorgelagerte Lücke – kann die zentrale Firewall dauerhaft und getarnt kompromittieren, eigene Programme einschleusen und den Zugang über Neustarts hinweg halten. Ein solcher Vorfall auf dem Perimeter-Gerät kann Datenabfluss, Betriebsunterbrechung und eine meldepflichtige Sicherheitsverletzung nach NIS-2 / DSGVO nach sich ziehen.

7,8 / 10

HOCH
CVSS 3.1 BASISWERT

`CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H` – setzt einen lokal authentifizierten Zugang voraus – wer ihn hat, kann über ein präpariertes Update-Paket ohne Integritätsprüfung beliebige Dateien und Code auf die Firewall bringen. Das NVD (NIST) bewertet die Lücke mit 7,8 (HOCH); Fortinet selbst stuft sie mit 3,3 (NIEDRIG) ein. Ausschlaggebend für die Dringlichkeit ist die von Fortinet bestätigte aktive Ausnutzung.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
10. Dezember 2021	FortiOS ≤ 6.0.13 · ≤ 6.2.9 · ≤ 6.4.7 · 7.0.0–7.0.2	Zeitnah

Das Wichtigste in 60 Sekunden.

7,8 · HOCH
CVSS-Schweregrad (3.1, NVD)

Lokal · Auth
Zugriff mit Anmeldung nötig

Aktiv
ausgenutzt · CISA KEV (seit 10.12.2021)

CWE-494
Download ohne Integritätsprüfung

Die Ursache: Der FortiOS-CLI-Befehl `execute restore src-vis` lädt ein Update-Paket, ohne dessen Integrität oder digitale Signatur zu prüfen (**CWE-494 – Download of Code Without Integrity Check**). Ein **lokal authentifizierter** Angreifer kann dadurch ein eigens präpariertes Paket unterschieben und über den Wiederherstellungs-Vorgang beliebige Dateien auf das Gerät schreiben. Der offizielle Fix beseitigt die Schwachstelle, indem der anfällige Befehl vollständig aus FortiOS entfernt wird.

ANGRIFFSKETTE

01
Authentifizierter Zugang – der Angreifer verfügt über einen Admin-/CLI-Zugang auf dem FortiGate (z. B. über gestohlene Zugangsdaten oder eine vorgelagerte Lücke)

02
Präpariertes Paket – Aufruf von `execute restore src-vis` mit einem manipulierten Update-Paket

03
Keine Prüfung – FortiOS lädt das Paket ohne Integritäts- oder Signaturkontrolle und schreibt beliebige Dateien auf das Gerät

04
Persistenz – fremde Dateien in `/data2/` und `/bin/`, unerwartete Prozesse und C&C-Verkehr zu externen IP-Adressen

Betroffenheit & Fixversionen

FortiOS-Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 6.0	≤ 6.0.13	6.0.14
FortiOS 6.2	≤ 6.2.9	6.2.10
FortiOS 6.4	≤ 6.4.7	6.4.8
FortiOS 7.0	7.0.0 – 7.0.2	7.0.3

Betroffen sind FortiOS-Stände unterhalb der genannten Fixversionen; FortiOS 7.2 und neuer sind im Advisory nicht als verwundbar geführt. Der Fix entfernt den Befehl `restore src-vis` vollständig – ein reines Update auf die Zielversion schließt die Lücke also zuverlässig. Da die Ausnutzung einen authentifizierten Zugang voraussetzt, ist die Härtung des Admin-Zugriffs (starke, rotierte Zugangsdaten, MFA, Trusted Hosts) eine wesentliche flankierende Maßnahme.

Regulatorischer Hinweis: Wird die Firewall über diese Schwachstelle kompromittiert und fließen dabei Zugangsdaten oder personenbezogene Daten ab, 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

07.12.2021
Fortinet veröffentlicht Advisory FG-IR-21-201, entfernt den Befehl und stellt Fixversionen bereit

10.12.2021
CISA nimmt CVE-2021-44168 in den KEV-Katalog auf – bestätigte aktive Ausnutzung

24.12.2021
KEV-Frist für US-Behörden zum Patchen

04.01.2022
NVD veröffentlicht den Eintrag (NIST-CVSS 3.1: 7,8 / HOCH, CWE-494)

Ihr Maßnahmenplan.

In dieser Reihenfolge – Admin-Zugang härten, patchen, auf Kompromittierung prüfen, im Verdachtsfall forensisch aufarbeiten.

SOFORT	KURZFRISTIG	BEI VERDACHT
Admin-Zugang härten / patchen	IoC-Abgleich auf dem Gerät	Forensik & Incident Response

01 Betroffenheit feststellen

Prüfen, welche FortiOS-Version im Einsatz ist. Betroffen sind alle Stände unterhalb `6.0.14 / 6.2.10 / 6.4.8 / 7.0.3`. Auch selten gewartete Außenstellen- und Reserve-Geräte einbeziehen.

02 Admin-Zugang härten (flankierend)

Da die Ausnutzung einen authentifizierten Zugang voraussetzt: administrativen Zugriff auf vertrauenswürdige Hosts/Netze begrenzen (Trusted Hosts), Mehr-Faktor-Authentisierung erzwingen und Admin-Zugangsdaten rotieren. So wird die Vorbedingung des Angriffs erschwert.

03 Patchen

Auf die jeweilige Fixversion oder neuer aktualisieren (`6.0.14 / 6.2.10 / 6.4.8 / 7.0.3`). Der Fix entfernt den anfälligen Befehl `restore src-vis` vollständig.

04 Auf Kompromittierung prüfen

Die von Fortinet genannten Indikatoren abgleichen: unerwartete Dateien in `/data2/` und `/bin/`, unbekannte laufende Prozesse sowie ausgehenden Verkehr zu fremden C&C-Adressen. Zusätzlich Admin-Login-Logs auf unerklärte Anmeldungen durchsehen.

05 Im Verdachtsfall forensisch aufarbeiten

Bestätigen sich Indikatoren, das Gerät als kompromittiert behandeln: aus vertrauenswürdiger Firmware neu aufsetzen, alle auf dem Gerät gespeicherten Geheimnisse (VPN-, Admin- und Dienst-Zugangsdaten) rotieren und den Vorfall dokumentieren. Ein Patch entfernt bereits platzierte Implantate nicht.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE DATEIEN

Unerwartete Dateien in `/data2/` und `/bin/`

PROZESSE

Unbekannte oder unerwartete laufende Prozesse auf dem FortiGate

NETZVERKEHR

Ausgehender C&C-Verkehr zu externen, unbekannten IP-Adressen

Zur Einordnung: Dies sind die von Fortinet im Advisory FG-IR-21-201 genannten Kompromittierungshinweise. Da die Ausnutzung über einen authentifizierten Zugang und einen regulären CLI-Vorgang läuft, ist zusätzlich die Auswertung der Admin-Authentifizierungs- und Konfigurations-Logs auf unerklärte Anmeldungen der zuverlässigste flankierende Indikator.

Wichtig: Der Fix beseitigt die Schwachstelle, indem der anfällige Befehl entfernt wird – er macht aber ein bereits platziertes Implantat nicht rückgängig. Wurde das Gerät vor dem Patch kompromittiert, bleibt der Angreifer-Zugang bestehen, bis das System aus vertrauenswürdiger Firmware neu aufgesetzt und alle Geheimnisse rotiert sind. Deshalb gehört die Kompromittierungsprüfung ebenso dazu 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: Anomale Admin-Anmeldungen an FortiGate-Systemen und ausgehender C&C-Verkehr von Firewalls fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden FortiGate-Systeme mit veralteten, ungepatchten FortiOS-Ständen 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-Systeme unverzüglich auf die jeweilige Fixversion (6.0.14 / 6.2.10 / 6.4.8 / 7.0.3) oder neuer aktualisieren.
- Administrativen Zugang härten lassen – Trusted Hosts, MFA und Rotation der Admin-Zugangsdaten, da der Angriff einen authentifizierten Zugang voraussetzt.
- Auf Kompromittierungs-Indikatoren prüfen lassen; bei Verdacht Forensik und Neuaufbau des Geräts – 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-2021-44168 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-21-201 (Removal of `restore src-vis` command, veröffentlicht 07.12.2021) · NVD (NIST-CVSS 3.1: 7,8 / HOCH, Vektor AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H; Fortinet-CNA-Bewertung 3,3 / NIEDRIG; CWE-494) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 10.12.2021, Frist 24.12.2021).
Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.