AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2022-41328

Path Traversal mit Datei-Lese/Schreibzugriff in Fortinet FortiOS.

Ein Angreifer mit Administrationsrechten kann in den betroffenen FortiOS-Versionen über speziell gestaltete CLI-Kommandos aus dem vorgesehenen Verzeichnis ausbrechen und beliebige Dateien auf dem zugrundeliegenden Linux-System lesen und schreiben. In hochgezielten Angriffen auf Behörden wurde die Lücke – verkettet mit einer kompromittierten FortiManager-Instanz – genutzt, um die FortiGate-Firmware zu manipulieren und ein dauerhaftes Implantat zu verankern. Die Schwachstelle wurde als Zero-Day ausgenutzt und steht im CISA-KEV-Katalog.

Geschäftsrisiko: Manipulation der Firewall auf Firmware-Ebene und dauerhafte, schwer erkennbare Hintertüren mit Fernzugriff – mit Potenzial für Umgehung der Perimeter-Sicherheit, Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

7,1 / 10

HOCH
CVSS 3.1 BASISWERT

`CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N` – lokal und mit Administrationsrechten – ein privilegierter Angreifer kann über präparierte CLI-Kommandos beliebige Dateien auf dem zugrundeliegenden Linux-System der Firewall lesen und schreiben, mit hoher Auswirkung auf Vertraulichkeit und Integrität. Fortinet bewertet die Lücke im eigenen Advisory mit 6,5 (mittel).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
März 2023 (Zero-Day)	FortiOS 7.2.0–7.2.3 / 7.0.0–7.0.9 FortiOS 6.4.0–6.4.11 / 6.2.0–6.2.13 / 6.0 (alle)	Sofort

Das Wichtigste in 60 Sekunden.

7,1 · HOCH
CVSS-Schweregrad (3.1, NVD)

Datei R/W
als Admin beliebig auf dem OS

Aktiv
ausgenutzt · CISA KEV (seit 14.03.2023)

CWE-22
Path Traversal

Die Ursache: FortiOS prüft in den betroffenen Versionen die Pfadangaben bestimmter CLI-Kommandos nicht ausreichend (CWE-22). Ein Angreifer mit **Administrationsrechten** kann dadurch aus dem vorgesehenen Verzeichnis ausbrechen und beliebige Dateien auf dem zugrundeliegenden Linux-System der Firewall **lesen und schreiben** – bis hin zum Austausch von System- und Firmware-Bestandteilen. In den beobachteten Angriffen wurde die Lücke mit einer kompromittierten `FortiManager`-Instanz verkettet, über die die Kommandos an die verwalteten FortiGate-Geräte ausgeführt wurden.

ANGRIFFSKETTE

01
Privilegierter Zugang – in den beobachteten Angriffen über eine kompromittierte FortiManager-Instanz, die Skripte auf verwaltete FortiGate-Geräte ausführt

02
Path Traversal auslösen – präparierte CLI-Kommandos brechen aus dem Verzeichnis aus und schreiben beliebige Dateien auf das Linux-System

03
Firmware manipulieren – `/sbin/init` wird so verändert, dass vor dem Boot das Implantat `/bin/fgfm` startet

04
Persistenz & C2 – `/bin/fgfm` wartet auf einen ICMP-Trigger, öffnet eine Reverse-Shell zum Command-and-Control-Server, exfiltriert Daten und erlaubt Fernsteuerung

Betroffenheit & Fixversionen

FortiOS-Version	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.2.x	`7.2.0 – 7.2.3`	`7.2.4`
FortiOS 7.0.x	`7.0.0 – 7.0.9`	`7.0.10`
FortiOS 6.4.x	`6.4.0 – 6.4.11`	`6.4.12`
FortiOS 6.2.x	`6.2.0 – 6.2.13`	`6.2.14`
FortiOS 6.0.x	`alle Versionen`	kein Fix (EoL) – Migration

Betroffen sind FortiOS 7.2.0–7.2.3, 7.0.0–7.0.9, 6.4.0–6.4.11, 6.2.0–6.2.13 sowie sämtliche Versionen des Zweigs 6.0. Für den End-of-Life-Zweig 6.0 stellt Fortinet keinen Fix bereit – hier ist die Migration auf einen unterstützten, korrigierten Zweig erforderlich. Die Ausnutzung setzt einen privilegierten Zugang voraus; in der beobachteten Kampagne wurde dieser über eine kompromittierte FortiManager-Instanz erlangt.

Regulatorischer Hinweis: Firewalls sind zentrale Sicherheitskomponenten – eine bestätigte Firmware-Manipulation 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.

ZEITACHSE

07.03.2023
CVE-2022-41328 · Überblick
Fortinet veröffentlicht Advisory FG-IR-22-369 mit Analyse der

09.03.2023
Fortinet-PSIRT-Blog beschreibt Angriffskette, das /bin/fgfm-

14.03.2023
CISA nimmt CVE-2022-41328 in den KEV-Katalog auf –

04.04.2023
KEV-Frist für US-Behörden zum Patchen/Mitigieren

Seite 3: Ihr Maßnahmenplan →

Ihr Maßnahmenplan.

In dieser Reihenfolge – Verwaltungszugang abschotten, patchen, Firmware-Integrität prüfen, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Verwaltungszugang abschotten /	Firmware-Integrität & IoCs prüfen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Prüfen, ob FortiOS in einer der betroffenen Versionen (7.2.0–7.2.3, 7.0.0–7.0.9, 6.4.0–6.4.11, 6.2.0–6.2.13 oder 6.0.x) im Einsatz ist und welche Geräte über eine FortiManager-Instanz zentral verwaltet werden.

02 Sofort mitigieren (vor dem Patch)

Administrativen Zugriff und die FortiManager-Anbindung strikt absichern: Verwaltungsschnittstelle aus nicht vertrauenswürdigen Netzen nehmen, Zugriff per `trusted hosts` / local-in policy auf autorisierte Hosts begrenzen und die Integrität der FortiManager-Instanz überprüfen.

03 Patchen

Auf einen korrigierten Stand aktualisieren: FortiOS `7.2.4`, `7.0.10`, `6.4.12` oder `6.2.14` bzw. neuer. Der End-of-Life-Zweig 6.0 erhält keinen Fix – hier auf einen unterstützten, korrigierten Zweig migrieren.

04 Firmware-Integrität prüfen

Auf Anzeichen einer Firmware-Manipulation prüfen: das Implantat `/bin/fgfm`, eine veränderte `/sbin/init`, die von Fortinet veröffentlichten Datei-Hashes sowie die FIPS-Fehlermeldung `Firmware Integrity self-test failed`. Die von Fortinet genannten Log- und Netz-IoCs abgleichen.

05 Kompromittierung behandeln

Bei Anzeichen einer Manipulation das Gerät als vollständig kompromittiert behandeln: Fortinet-Support einbinden, aus einer vertrauenswürdigen Firmware sauber neu aufsetzen, Konfiguration gegen einen bekannt-guten Stand abgleichen und alle Administrator-Zugangsdaten sowie Schlüssel rotieren – ein Patch entfernt eine bereits verankerte Firmware-Hintertür nicht.

Kompromittierungs-Indikatoren (IoCs)

IMPLANTAT / FIRMWARE

Datei `/bin/fgfm` und modifizierte `/sbin/init` auf dem Gerät

NETZ-IOC

C2-Kontakt zu `47.252.20.90`

ICMP-Trigger `_;7(Zu9YTsA7qQ#vm`

INTEGRITÄTSWARNUNG

FIPS-Geräte melden `Firmware Integrity self-test failed`

Zur Einordnung: Fortinet hat im PSIRT-Blog Datei-Hashes für die Implantate (u. a. fgfm, auth, klogd) sowie die genannten Log- und Netzindikatoren veröffentlicht. FIPS-fähige Geräte erkennen die Firmware-Manipulation automatisch und wechseln in einen Fehlerzustand; auf Geräten ohne FIPS ist der Abgleich der Dateien und Hashes gegen einen bekannt-guten Stand der zuverlässigste Indikator.

Wichtig: Der Kern des Risikos liegt in der Persistenz auf Firmware-Ebene: Hat ein Angreifer die Lücke genutzt, um /sbin/init zu verändern und /bin/fgfm zu verankern, bleibt der Zugang auch nach dem Patch bestehen. Ein bloßes Update genügt dann nicht – ein kompromittiertes Gerät muss aus vertrauenswürdiger Firmware neu aufgesetzt 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: Firmware-Integritätsanomalien, das Implantat /bin/fgfm, ICMP-getriggerte Reverse-Shells und C2-Verbindungen zu 47.252.20.90 fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden ungepatchte FortiOS-Geräte mit erreichbarer Verwaltungs-/CLI-Schnittstelle oder zentraler FortiManager-Anbindung 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

- Verwaltungszugang der FortiGate-Geräte und die FortiManager-Anbindung heute absichern; Patch auf 7.2.4 / 7.0.10 / 6.4.12 / 6.2.14 unverzüglich einplanen, 6.0-Geräte migrieren.
- Firmware-Integrität jedes betroffenen Geräts gegen die von Fortinet veröffentlichten IoCs prüfen lassen.
- Bei Anzeichen einer Manipulation das Gerät sauber neu aufsetzen und Zugangsdaten rotieren – 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-2022-41328 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-22-369 und PSIRT-Analyse-Blog (Angriffskette, /bin/fgfm-Implantat, IoCs) · NVD (CVSS 3.1: 7,1 / AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N, CWE-22; Fortinet-eigene Bewertung 6,5 / mittel) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 14.03.2023, Frist 04.04.2023). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.