AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2019-6693

Fest einprogrammierter Schlüssel in Fortinet FortiOS-Konfiguration.

FortiOS, FortiManager und FortiAnalyzer verschlüsseln vertrauliche Werte in der CLI-Konfiguration mit einem fest einprogrammierten, allgemein bekannten Schlüssel. Wer Zugriff auf eine Konfigurationssicherung oder die exportierte CLI-Konfiguration erlangt, kann damit Nutzerpasswörter, VPN- und HA-Geheimnisse sowie Passphrasen privater Schlüssel im Klartext wiederherstellen – und die erbeuteten Zugangsdaten anschließend gegen das Netz wenden. Die Schwachstelle steht seit Juni 2025 im CISA-KEV-Katalog und wird unter anderem von der Akira-Ransomware-Gruppe zur Erstinfektion genutzt.

Geschäftsrisiko: Aus einer scheinbar harmlosen Konfigurationssicherung werden verwertbare Zugangsdaten: VPN-Passwörter, HA-Geheimnisse und Nutzerkennwörter können entschlüsselt und für unbefugten Netzzugriff, laterale Ausbreitung und Ransomware-Erstinfektion missbraucht werden – mit Potenzial für Betriebsunterbrechung, Datenabfluss und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

6,5 / 10

MITTEL
CVSS 3.1 BASISWERT

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N` – Wer eine Konfigurationssicherung oder die CLI-Konfiguration in die Hände bekommt, kann mit dem allgemein bekannten, fest einprogrammierten Schlüssel sämtliche darin als „ENC“ gespeicherten Geheimnisse entschlüsseln – ohne weiteren Aufwand. Fortinet selbst bewertet die Lücke mit 4,2 (CVSS 3.1).

AUSGENUTZT SEIT
25. Juni 2025 (CISA KEV)

BETROFFEN
FortiOS ≤ 5.6.10, 6.0.0–6.0.6, 6.2.0
FortiManager ≤ 6.2.4 · FortiAnalyzer ≤ 6.2.3

HANDLUNGSBEDARF
Hoch

Das Wichtigste in 60 Sekunden.

6,5 · MITTEL
CVSS-Schweregrad (3.1 / NVD)

Hardcoded Key
Config-Geheimnisse entschlüsselbar

Aktiv
ausgenutzt · CISA KEV (seit 25.06.2025)

CWE-798
Use of Hard-coded Credentials

Die Ursache: In den betroffenen Versionen verschlüsselt FortiOS die als `ENC` markierten Geheimnisse in der CLI-Konfiguration mit einem **fest im Code hinterlegten symmetrischen Schlüssel** (in `fips.c`). Da dieser Schlüssel in allen Geräten identisch und allgemein bekannt ist, bietet die Verschlüsselung keinen echten Schutz: Ein Angreifer mit Zugriff auf die CLI-Konfiguration oder eine Konfigurationssicherung kann die darin gespeicherten Geheimnisse ohne Anmeldedaten wieder in Klartext überführen.

ANGRIFFSKETTE

01
Konfiguration erlangen – Zugriff auf eine Konfigurationssicherung oder die exportierte CLI-Konfiguration (Backup-Ablage, Fehlkonfiguration, unsicherer Transportweg)

02
Bekannter Schlüssel – der fest einprogrammierte, geräteübergreifend identische Schlüssel ist öffentlich bekannt

03
Geheimnisse entschlüsseln – Nutzerpasswörter, VPN- und HA-Geheimnisse sowie Passphrasen privater Schlüssel im Klartext (Ausnahme: Administrator-Passwort in FortiOS)

04
Ausweitung – wiederverwendete Zugangsdaten für Netzzugriff, laterale Bewegung und Ransomware-Erstinfektion (u. a. Akira)

Betroffenheit & Fixversionen

Produkt / Version	Verwundbar bis	Fixversion (Ziel)
FortiOS 5.6.x	≤ 5.6.10	5.6.11
FortiOS 6.0.x	6.0.0 – 6.0.6	6.0.7
FortiOS 6.2.x	6.2.0	6.2.1
FortiManager	≤ 6.2.4	6.2.5
FortiAnalyzer	≤ 6.2.3	6.2.4

Betroffen sind FortiOS in den genannten Versionsständen sowie FortiManager ≤ `6.2.4` und FortiAnalyzer ≤ `6.2.3`. Der eigentliche Schaden entsteht nicht auf dem Gerät selbst, sondern überall dort, wo eine Konfigurationssicherung liegt – in Backup-Systemen, Ticket-Anhängen, E-Mails oder auf Administrator-Arbeitsplätzen. Jede solche Kopie ist so schützenswert wie die darin enthaltenen Geheimnisse selbst.

Regulatorischer Hinweis: Werden über abgeflossene Konfigurationsdaten Zugangsdaten oder personenbezogene Daten kompromittiert, kann dies 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

FG-IR-19-007
CVE-2019-6693 · Überblick
Fortinet-Advisory mit Fixes in FortiOS 5.6.11 / 6.0.7 / 6.2.1

25.06.2025
CISA nimmt CVE-2019-6693 in den KEV-Katalog auf – aktive

16.07.2025
KEV-Frist für US-Behörden zum Patchen/Mitigieren

2025
Akira-Ransomware nutzt die Schwachstelle zur Erstinfektion

Seite 3: Ihr Maßnahmenplan →

Ihr Maßnahmenplan.

In dieser Reihenfolge – patchen, Konfigurationssicherungen absichern, gespeicherte Geheimnisse rotieren, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Auf feste Version aktualisieren	Config-Backups absichern &	Zugriff auf alte Sicherungen prüfen

01 Betroffenheit feststellen

Prüfen, ob FortiOS in einer Version unterhalb `5.6.11` / `6.0.7` / `6.2.1` bzw. FortiManager ≤ `6.2.4` oder FortiAnalyzer ≤ `6.2.3` im Einsatz ist. Auch außer Betrieb genommene Geräte zählen, solange deren Konfigurationssicherungen noch irgendwo liegen.

02 Patchen

Auf eine feste Version aktualisieren: FortiOS `5.6.11`, `6.0.7` bzw. `6.2.1` oder neuer; FortiManager `6.2.5`+, FortiAnalyzer `6.2.4`+. Erst neuere Versionen verwenden einen geräteindividuellen Schlüssel.

03 Konfigurationssicherungen als sensibel behandeln

Alle vorhandenen Config-Backups aufspüren und absichern (Zugriff beschränken, verschlüsselt ablegen, aus Ticket-/E-Mail-Anhängen entfernen). Jede mit einer verwundbaren Version erstellte Sicherung enthält entschlüsselbare Geheimnisse – ein Patch macht diese Altkopien nicht sicher.

04 Gespeicherte Geheimnisse als kompromittiert behandeln

Alle in betroffenen Konfigurationen gespeicherten Geheimnisse rotieren: lokale Nutzerpasswörter, VPN- und IPsec-Pre-Shared-Keys, HA-Passwort sowie Passphrasen hinterlegter privater Schlüssel. Ein Update entwertet bereits abgeflossene Geheimnisse nicht.

05 Kompromittierung ausschließen

VPN- und Admin-Authentifizierungslogs auf Anmeldungen mit potenziell abgeflossenen Konten prüfen und auf bekannte Akira-Indikatoren abgleichen. Nachvollziehen, wer in der Vergangenheit Zugriff auf Konfigurationssicherungen hatte.

Kompromittierungs-Indikatoren (IoCs)

PRIMÄRER ANSATZPUNKT	AUFFÄLLIGE AKTIVITÄT	FOLGEINDIKATOREN
Unkontrollierte Konfigurationssicherungen in Backups, Ticket-/Mail-Anhängen, auf Admin-Arbeitsplätzen	VPN-/Admin-Anmeldungen mit in der Config hinterlegten Konten aus fremden Quellen	Bekannte Akira-Ransomware-Indikatoren und laterale Bewegung nach VPN-Zugang

Zur Einordnung: Der Missbrauch ist auf dem Gerät selbst kaum sichtbar, da die Entschlüsselung offline am erbeuteten Konfigurationsstand erfolgt. Der zuverlässigste Indikator ist die Auswertung Ihrer VPN- und Authentifizierungslogs sowie die Nachverfolgung, welche Konfigurationssicherungen wem zugänglich waren.

Wichtig: Der Kern des Risikos liegt nicht im Gerät, sondern in seinen Konfigurationssicherungen: Der feste Schlüssel ist allgemein bekannt, deshalb schützt die Verschlüsselung dort gespeicherte Geheimnisse nicht. Sind VPN-, HA- oder Nutzergeheimnisse einmal aus einer Altsicherung entschlüsselt, bleibt der Zugang auch nach dem Patch bestehen. Die Rotation aller betroffenen Geheimnisse ist daher 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: Nutzung aus alten Konfigurationen entschlüsselter VPN-/Admin-Zugangsdaten sowie bekannte Akira-Ransomware-Indikatoren fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden verwundbare FortiOS-/FortiManager-/FortiAnalyzer-Stände und deren zugängliche Konfigurationssicherungen 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 FortiOS-/FortiManager-/FortiAnalyzer-Stände unverzüglich auf eine feste Version aktualisieren.
- Alle in verwundbaren Konfigurationen gespeicherten Geheimnisse (VPN-/HA-/Nutzerkennwörter, private Schlüssel) rotieren lassen und Altsicherungen absichern.
- Prüfen lassen, ob bereits abgeflossene Zugangsdaten genutzt wurden – 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-2019-6693 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-19-007 (Fixes FortiOS 5.6.11 / 6.0.7 / 6.2.1, FortiManager 6.2.5, FortiAnalyzer 6.2.4; Herstellerwertung CVSS 3.1: 4,2) · NVD CVE-2019-6693 (CVSS 3.1: 6,5 MITTEL, Vektor AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N, CWE-798) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 25.06.2025, Frist 16.07.2025) · öffentlich berichtete Ausnutzung durch Akira-Ransomware. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.