AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-35616

Pre-Auth-API-Bypass in Fortinet FortiClient EMS.

Ein nicht authentifizierter Angreifer aus dem Netz kann die API-Zugriffskontrolle des zentralen FortiClient-EMS-Management-Servers vollständig umgehen und darüber Code bzw. Befehle ausführen. Über manipulierte Bereitstellungsprofile lassen sich Schadskripte an alle verwalteten Endpunkte ausspielen – aktuell genutzt, um den EKZ-Infostealer getarnt als Fortinet-Patch zu verteilen. Als Zero-Day seit Ende März 2026 ausgenutzt.

> **Geschäftsrisiko:** Übernahme der zentralen Endpunkt-Verwaltung – mit Potenzial für die Kompromittierung sämtlicher verwalteter Clients, Diebstahl von Zugangsdaten, Datenabfluss und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,8 / 10

KRITISCH
CVSS 3.1 BASISWERT

`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 des Nutzers, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Fortinet nennt zusätzlich einen zeitlich angepassten Wert von 9,1 (aktive Ausnutzung, Fix verfügbar).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
31. März 2026	FortiClient EMS 7.4.5 – 7.4.6 Cloud & FortiSASE bereits gepatcht	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-3.1-Basiswert

Pre-Auth
API-Bypass · Codeausführung ohne Anmeldung

Aktiv
als Zero-Day ausgenutzt · CISA KEV

> 2.000
exponierte EMS-Server · viele in Deutschland

Die Ursache: FortiClient EMS prüft bei bestimmten API-Aufrufen die Authentifizierung und Autorisierung unzureichend (CWE-284, Improper Access Control). Speziell präparierte Anfragen umgehen die Zugriffskontrolle vollständig, sodass ein nicht authentifizierter Angreifer privilegierte Funktionen aufrufen und Code bzw. Befehle auf dem Management-Server ausführen kann. Da EMS die verwalteten Endpunkte steuert, wirkt eine Kompromittierung des Servers auf die gesamte Client-Flotte.

ANGRIFFSKETTE

01
API-Bypass – präparierte Anfragen umgehen die Authentifizierung des EMS-Servers

02
Profil manipulieren – das Remote-Access-/Bereitstellungsprofil wird um ein Schadskript ergänzt

03
Ausspielen – verbundene FortiClient-Endpunkte führen das Skript automatisch aus und laden per PowerShell die Nutzlast

04
Infostealer – EKZ stiehlt Browser-Zugangsdaten und Cookies und exfiltriert sie per HTTP-POST

Betroffenheit & Fixversionen

FortiClient-EMS-Zweig	Verwundbar bis	Fixversion (Ziel)
7.4	`7.4.5 – 7.4.6`	`7.4.7 / Hotfix`
8.0	nicht betroffen	—
7.2 und älter	nicht betroffen	—
Cloud · FortiSASE	bereits gepatcht	keine Aktion nötig

Betroffen sind ausschließlich die On-Prem-Versionen `7.4.5` und `7.4.6`. Fortinet hat Hotfixes für beide Zweige bereitgestellt; die finale Korrektur folgt mit dem angekündigten Release `7.4.7`. Cloud- und FortiSASE-Instanzen sind bereits herstellerseitig gepatcht. Exakten Hotfix-Build gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff oder Abfluss von Zugangsdaten 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

31.03.2026
Als Zero-Day ausgenutzt beobachtet und an Fortinet gemeldet

04.04.2026
Fortinet veröffentlicht Advisory FG-IR-26-099 + Hotfixes

06.04.2026
CISA KEV · Behörden-Frist 09.04.2026

Seither
Aktiv ausgenutzt – EKZ-Infostealer getarnt als Fortinet-Patch

Ihr Maßnahmenplan.

In dieser Reihenfolge – Exposition kappen vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
EMS-Verwaltung abschotten	Hotfix einspielen	Endpunkte auf Kompromittierung prüfen

01 Betroffenheit feststellen

Installierte FortiClient-EMS-Version prüfen: Nur On-Prem `7.4.5` und `7.4.6` sind angreifbar; `7.2` und älter sowie `8.0` nicht. Zusätzlich klären, ob die EMS-Verwaltungsschnittstelle aus dem Internet erreichbar ist – das erhöht die Dringlichkeit erheblich.

02 Sofort abschotten (vor dem Patch)

Die EMS-Verwaltungs- und API-Schnittstelle vom Internet trennen bzw. nur über VPN/administratives Netz erreichbar machen, bis der Hotfix eingespielt ist. Damit entfällt der unauthentifizierte Zugriffspfad.

03 Patchen

Den Hotfix für den eigenen Zweig (`7.4.5` bzw. `7.4.6`) einspielen oder auf `7.4.7` aktualisieren, sobald verfügbar. Build-Nummer gegen FG-IR-26-099 abgleichen.

04 Kompromittierung ausschließen

Bereitstellungs- und Remote-Access-Profile in EMS auf unbekannte oder nachträglich eingefügte Skripte prüfen. Verwaltete Endpunkte auf die IoCs unten abgleichen – insbesondere `FortiEndpoint_Patch.exe`, das Skript-Verzeichnis und `log.txt`. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Endpunkte bereinigen

Bei Fund den EKZ-Infostealer entfernen, betroffene Browser-Zugangsdaten und Cookies als kompromittiert behandeln und Passwörter zurücksetzen. Für zentrale/privilegierte Konten priorisiert vorgehen.

Kompromittierungs-Indikatoren (IoCs)

DATEIEN

lokal `FortiEndpoint_Patch.exe` · Download `p.exe`

SHA-256

`0da123adf9251957a4b850a3f6bd6a753dd4892be176a84a18450e899534cc5e`

NETZ-MARKER

`83.138.53.110` (Delivery + Exfil)

Tor-Exit `185.220.101.15` · `192.42.116.14`

`hxxp://83.138.53.110/dl/p.exe`

`hxxp://83.138.53.110/service/save.php`

DA

`C:`

`Fi`

`C:`

Zur Einordnung: IPs, URLs und Dateinamen sind eine Momentaufnahme der beobachteten EKZ-Kampagne und flüchtig – kein Ersatz für die Prüfung Ihrer EMS-Bereitstellungsprofile und Endpunkt-Logs. Der zuverlässigste Frühindikator sind unerwartete Änderungen an Remote-Access-/Deployment-Profilen und daraus ausgelöste PowerShell-Downloads.

Wichtig: Weil EMS Code an die verwalteten Endpunkte ausspielt, breitet sich eine Server-Kompromittierung auf die gesamte Client-Flotte aus. Die Schadsoftware kommt getarnt als legitimer Fortinet-Patch (FortiEndpoint_Patch.exe) – Nutzer schöpfen keinen Verdacht.

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: Unerwartete Änderungen an Bereitstellungsprofilen und daraus ausgelöste PowerShell-Downloads auf Endpunkten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Internet erreichbare, ungepatchte FortiClient-EMS-Server 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 Fortinet-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

- EMS-Verwaltung heute vom Internet abschotten, Hotfix innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob Profile manipuliert und Endpunkte bereits kompromittiert wurden – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung der Management-Systeme und des Perimeters entscheiden.

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-2026-35616 und dem Fortinet-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-26-099 (CVE-2026-35616) · NVD · CISA Known Exploited Vulnerabilities Catalog · Arctic Wolf Labs · BleepingComputer · watchTowr. Angaben nach bestem Wissen zum Stand 14.07.2026; Hotfix-Builds und die finale Fixversion 7.4.7 gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.