THREAT INTELLIGENCE BRIEFING

CVE-2026-121529

Codeausführung über die lokale Schnittstelle von FortiClient.

Die lokale Programmierschnittstelle von FortiClient prüft nicht ausreichend, woher Anfragen kommen. Ein Angreifer ohne Anmeldung kann dadurch auf dem Endgerät Code oder Befehle ausführen, wenn das Opfer dabei mitwirkt. Fortinet hat die Lücke am 10.11.2026 mit FortiClient 7.4.8 und 7.2.15 geschlossen; eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** Codeausführung auf Mitarbeiter-Endgeräten mit installiertem VPN-Client – mit Potenzial für Rechteausweitung, Zugangsdatendiebstahl, Einstieg ins Firmennetz und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

9,6 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H` – aus dem Netz, ohne Rechte, mit einer Handlung des Opfers, mit voller Wirkung über das betroffene Programm hinaus. Basiswert laut NVD (Vektor von Fortinet als CNA); Fortinet weist inkl. Zeitfaktoren 9,1 aus.

AUSNUTZUNG
Nicht bekannt (Stand 10.11.2026)

BETROFFEN
FortiClient 7.4.0–7.4.7
Windows auch 7.2.0–7.2.14

HANDLUNGSBEDARF
Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,6 · KRITISCH
CVSS-Schweregrad

Origin-Prüfung
lokale API-Schnittstelle · CWE-346

Nicht bekannt
Ausnutzung · nicht in CISA KEV · kein PoC öffentlich

7.4.8 · 7.2.15
Fixversionen seit 10.11.2026

Die Ursache: FortiClient stellt auf dem Endgerät eine **lokale API-Schnittstelle** bereit. Diese prüft die Herkunft eingehender Anfragen nicht ausreichend (**CWE-346, Origin Validation Error**). Ein nicht authentifizierter Angreifer kann dadurch aus der Ferne Code oder Befehle ausführen lassen, Voraussetzung ist eine Handlung des Opfers. Fortinet ordnet die Auswirkung als Rechteausweitung ein und nennt keine weiteren technischen Details.

ANGRIFFSKETTE

01	02	03	04
Client installiert – verwundbarer FortiClient läuft auf dem Endgerät	**Opfer handelt** – Nutzer führt eine vom Angreifer gesteuerte Aktion aus	**API missbraucht** – Anfrage fremder Herkunft wird angenommen	**Codeausführung** – Befehle auf dem Endgerät, Rechteausweitung

Betroffenheit & Fixversionen

Produkt · Zweig	Verwundbar bis	Fixversion (Ziel)
Windows 7.4	7.4.0 bis 7.4.7	7.4.8
Windows 7.2	7.2.0 bis 7.2.14	7.2.15
Mac 7.4	7.4.0 bis 7.4.7	7.4.8
Windows PAM	bis 7.4.7 / 7.2.14	7.4.8 / 7.2.15
8.0 · Mac 7.2	nicht betroffen	—

Angaben laut Fortinet-Advisory FG-IR-26-194. Fortinet nennt **keinen Workaround** und keinen virtuellen Patch. Die Ausnutzung setzt eine Interaktion des Opfers voraus. Das CVE-Record nennt für Windows PAM nur 7.4.7 und 7.2.14, das Advisory die vollen Zweige – maßgeblich ist das Advisory.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf Endgeräte mit personenbezogenen Daten 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

03.11.2026
CVE-Nummer reserviert

10.11.2026
FG-IR-26-194 · Fix 7.4.8 / 7.2.15

10.11.2026
CISA: keine Ausnutzung bekannt

Stand heute
Nicht in CISA KEV · kein PoC

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Inventar vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Client-Versionen erfassen	Update verteilen	Endgeräte beobachten

01 Betroffenheit feststellen

Über EMS oder Softwareinventar alle FortiClient-Installationen erfassen: Windows `7.2.0`–`7.2.14` und `7.4.0`–`7.4.7`, Mac `7.4.0`–`7.4.7`, Windows PAM in denselben Zweigen. Version 8.0 ist nicht betroffen.

02 Patchen

Auf `7.4.8` bzw. `7.2.15` oder auf 8.0 aktualisieren, zentral über EMS verteilen. Mobile und selten verbundene Geräte gezielt nachverfolgen.

03 Risiko bis zum Update senken

Fortinet nennt keinen Workaround. Nutzer auf die Lücke hinweisen und Endgeräte mit veralteter Version priorisiert aktualisieren, zuerst Administratoren und Mitarbeitende mit privilegierten Zugängen.

04 Kompromittierung ausschließen

EDR-Daten auf ungewöhnliche Kindprozesse der FortiClient-Dienste prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Fortinet nennt keine, Ausnutzung nicht bekannt

AUSWERTUNGSQUELLEN

EDR-Telemetrie der Endgeräte
FortiClient-/EMS-Logs

AUFFÄLLIGE MUSTER

Shell- oder Skriptprozesse unter FortiClient-Diensten
unerwartete Konfigurationsänderungen am Client

Zur Einordnung: Es liegen keine CVE-spezifischen Indikatoren vor. Die genannten Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

Wichtig: Der VPN-Client läuft auf vielen Geräten mit hohen Rechten und wird selten aktiv überwacht. Ohne Endgeräte-Erkennung bleibt ein Missbrauch der Client-Schnittstelle unsichtbar.

Bildmotive: KI-generierte Symbolbilder

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: Ein Shell-Prozess, der von einem FortiClient-Dienst gestartet wird fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden Endgeräte mit veraltetem FortiClient 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 FortiClient-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

- Update aller FortiClient-Installationen auf 7.4.8 bzw. 7.2.15 anordnen.
- Vollständigkeit des Client-Inventars bestätigen lassen.
- Über eine dauerhafte Überwachung der Endgeräte 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-2026-121529 und dem FortiClient-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Fortinet PSIRT FG-IR-26-194 (10.11.2026, Fixversionen, CVSS 9,1 inkl. Zeitfaktoren) · NVD (CVSS 3.1 Basiswert 9,6) · CVE-Eintrag mit CISA-ADP-SSVC (Exploitation: none, Automatable: no) · CISA KEV (Stand 10.11.2026: nicht gelistet). Stand 10.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.