AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-1340

Unauthentifizierte Codeausführung in Ivanti Endpoint Manager Mobile.

Ein nicht authentifizierter Angreifer aus dem Internet kann über einen einzigen präparierten HTTP-Aufruf beliebige Betriebssystembefehle mit Root-Rechten auf dem EPMM-Server ausführen – ohne Zugangsdaten und ohne Nutzerinteraktion. Die Lücke wurde als Zero-Day ausgenutzt, bevor Ivanti sie am 29. Januar 2026 öffentlich machte; CISA führt sie seit dem 8. April 2026 als aktiv ausgenutzt.

> **Geschäftsrisiko:** die vollständige Übernahme des zentralen Mobile-Device-Management-Servers – mit Zugriff auf Geräte- und Personendaten der gesamten Mobilflotte (u. a. PII, Telefonnummern, Standortdaten, Geräte-IDs), Persistenz und lateraler Bewegung ins interne Netz. Ein bestätigter Zugriff ist ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO.

9,8 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`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 – vollständiger Verlust von Vertraulichkeit, Integrität und Verfügbarkeit. Von Ivanti mit dem oberen Höchstbereich bewertet.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
vor dem 29.01.2026 (Zero-Day)	EPMM ≤ 12.7.0.0 (alle Zweige bis 12.7)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Pre-Auth RCE
unauth. Codeausführung als root

Aktiv
Zero-Day · CISA KEV · PoC öffentlich

MDM-Server
volle Kontrolle über die Geräteflotte

Die Ursache: Die verwundbaren EPMM-Versionen verarbeiten die von Apache über `RewriteMap` aufgerufenen Bash-Skripte `map-appstore-url` und `map-aft-store-url` unsicher. Ein von außen steuerbarer Wert (Parameter `h`) landet in einem arithmetischen Auswertungskontext. Bash expandiert dabei einen Array-Index mit Kommando-Substitution – ein in Backticks oder Klammern verpackter Befehl wird mit **Root-Rechten** ausgeführt. Authentifizierung ist nicht erforderlich, der Endpunkt ist vorauthentifiziert erreichbar.

ANGRIFFSKETTE

01
Portal exponiert – der EPMM-Dienst (`/mifs`) ist aus dem Internet erreichbar

02
Request senden – HTTP-GET an `/mifs/c/appstore/fob/...` mit präpariertem `h`-Parameter

03
Bash-Injection – Kommando im Array-Index wird per arithmetischer Expansion ausgewertet

04
Root-Zugriff – beliebige OS-Befehle mit Root-Rechten auf dem MDM-Server

Betroffenheit & Fixversionen

EPMM-Zweig	Verwundbar bis	Fixversion (Ziel)
12.5.0.0	≤ 12.5.0.0	RPM 12.x.0.x
12.6.0.0	≤ 12.6.0.0	RPM 12.x.0.x
12.7.0.0	≤ 12.7.0.0	RPM 12.x.0.x
12.5.1.0	≤ 12.5.1.0	RPM 12.x.1.x
12.6.1.0	≤ 12.6.1.0	RPM 12.x.1.x
Permanenter Fix	alle Zweige	12.8.0.0 (angekündigt)

Ivanti stellt zunächst temporäre RPM-Hotfixes bereit: Zweige mit Endung `.0.0` erhalten RPM `12.x.0.x`, Zweige mit Endung `.1.0` erhalten RPM `12.x.1.x`. Der permanente Fix `12.8.0.0` ist angekündigt (Q1 2026), der Release-Stand ließ sich zum Redaktionsschluss nicht abschließend verifizieren. Exakte Patch-Zuordnung gegen das Ivanti-Advisory des eigenen Zweigs abgleichen.

Regulatorischer Hinweis: Die Übernahme des MDM-Servers bedeutet potenziellen Zugriff auf personenbezogene Daten der verwalteten Endgeräte. Ein bestätigter Zugriff 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

29.01.2026
Ivanti veröffentlicht Advisory (CVE-2026-1281 und CVE-

29.01.2026
Bereits als Zero-Day vor Veröffentlichung ausgenutzt

30.01.2026
Öffentliche technische Analysen und PoC (watchTowr,

08.04.2026
CISA nimmt CVE-2026-1340 in den KEV-Katalog auf · Frist

Ihr Maßnahmenplan.

In dieser Reihenfolge – Patch vor Entwarnung, Threat Hunting parallel.

SOFORT	SOFORT	PARALLEL
RPM-Hotfix einspielen	Exposition einschränken	Threat Hunting / Log-Abgleich

01 Betroffenheit feststellen

EPMM-Version ermitteln – betroffen ist jede Version bis einschließlich `12.7.0.0` (beide Zweig-Familien `.0.0` und `.1.0`). Prüfen, ob der Dienst (`/mifs`) aus dem Internet erreichbar ist – exponierte Instanzen sind höchste Priorität.

02 Sofort patchen (Notfallverfahren)

Den RPM-Hotfix des eigenen Zweigs außerhalb des regulären Patch-Zyklus einspielen: `RPM 12.x.0.x` für `.0.0`-Zweige, `RPM 12.x.1.x` für `.1.0`-Zweige. Da bereits aktiv ausgenutzt wird, ist die Ausnutzung trivial – kein Aufschub.

03 Exposition reduzieren

Bis zum Patch den Zugriff auf das EPMM-Portal über Access-Control / WAF einschränken und die Endpunkte `/mifs/c/appstore` und `/mifs/c/aftstore` filtern bzw. sperren, sofern diese Funktionen nicht benötigt werden.

04 Kompromittierung ausschließen

Die httpd-Access-Logs auf GET-Requests an die genannten `/mifs`-Endpunkte mit auffälliger `h`-Parameter-Syntax (Backticks, Klammern) durchsuchen und das Dateisystem, insbesondere `/mi/`, auf untergeschobene Dateien prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Auf permanenten Fix planen

Den permanenten Fix `12.8.0.0` einplanen, sobald für Ihre Umgebung freigegeben, und den Release-/Support-Status direkt mit Ivanti abstimmen. Herstellerseitige Erkennungs-/IPS-Signaturen einspielen, sofern verfügbar.

Kompromittierungs-Indikatoren (IoCs)

VERWUNDBARE ENDPUNKTE (GET)

`/mifs/c/appstore/fob/…`
`/mifs/c/aftstore/fob/…`

AUFFÄLLIGE MARKER

`h`-Parameter mit Backticks/Klammern, z. B. `gPath[`…`]`
unerwartete Dateien unter `/mi/`

LOG-HINWEIS (HTTPD ACCESS LOG)

GET auf `/mifs/c/(app|aft)store` mit `theValue??`-Muster

Zur Einordnung: Belastbare öffentliche Angreifer-IPs lagen zum Redaktionsschluss nicht vor – die Endpunkte sind reguläre EPMM-Aufrufe, auffällig ist allein die injizierte Parameter-Syntax. Kein Ersatz für die Analyse Ihrer eigenen HTTP-Zugriffs-Logs und des Dateisystems.

Wichtig: Erfolgreiche Ausnutzung erscheint als regulärer HTTP-GET in den Zugriffs-Logs – ohne Alarm. Der Angreifer erlangt Root-Rechte und kann Persistenz einrichten; ohne Log- und Dateisystem-Analyse bleibt ein bereits erfolgter Zugriff unsichtbar.

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 GET-Requests auf die /mifs-Appstore-Endpunkte sowie neue Root-Prozesse oder -Dateien auf dem EPMM-Server 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 EPMM-Portale 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 Ivanti EPMM-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

- RPM-Hotfix des eigenen EPMM-Zweigs im Notfallverfahren heute einspielen.
- Prüfen lassen, ob der MDM-Server bereits kompromittiert wurde – dokumentiert für eine etwaige Meldung.
- EPMM-Exposition zum Internet dauerhaft einschränken und überwachen lassen.

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-2026-1340 und dem Ivanti EPMM-Perimeter.

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

Termin buchen

Quellen: Ivanti Security Advisory EPMM CVE-2026-1281 und CVE-2026-1340 · NVD (NIST) CVE-2026-1340 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 08.04.2026, Frist 11.04.2026) · Rapid7 Emergent Threat Report · watchTowr Labs Analyse · Tenable Research. Angaben nach bestem Wissen zum Stand 14.07.2026; Fix-/Patch-Zuordnung gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.