AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-1281

Unauthentifizierte Codeausführung in Ivanti Endpoint Manager Mobile.

Ein nicht authentifizierter Angreifer aus dem Internet kann über eine präparierte HTTP-Anfrage an das EPMM-Portal beliebige Betriebssystem-Befehle ausführen – ohne Anmeldung, ohne Nutzerinteraktion. Ivanti bestätigt eine Ausnutzung als Zero-Day bereits vor der Veröffentlichung; seit dem 30.01.2026 ist ein funktionierender Exploit öffentlich.

> **Geschäftsrisiko:** vollständige Übernahme des Mobile-Device-Management-Servers – mit Zugriff auf personenbezogene Gerätedaten (Namen, E-Mail, Rufnummern, GPS) und dem Potenzial für Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen 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 der Nutzer, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD-Basiswert nach CVSS 3.1.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
vor Veröffentlichung (Zero-Day, vor 29.01.2026)	EPMM ≤ 12.7.0.0 (alle unterstützten Zweige)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Pre-Auth RCE
unauth. Codeausführung

Zero-Day
aktiv ausgenutzt · CISA KEV · PoC öffentlich

≤ 12.7.0.0
alle EPMM-Zweige betroffen

Die Ursache: Ältere Bash-Skripte, die der Apache-Webserver von EPMM zum URL-Rewriting nutzt, werten Teile der URL ungeprüft in einer Bash-Umgebung aus. Über die **Arithmetik-Expansion** von Bash lässt sich in den Hash-Parameter einer Download-URL Code einschleusen (z. B. `gPath[`<befehl>`]`). Der eingebettete Befehl wird bei der Auswertung des Ausdrucks mit den Rechten des Webdienstes ausgeführt – ohne jede Authentifizierung.

ANGRIFFSKETTE

01
Portal exponiert – EPMM ist aus dem Internet erreichbar

02
Server prüfen – Testbefehl (z. B. `sleep`) verrät die Verwundbarkeit an der Antwortzeit

03
Befehl einschleusen – Bash-Code im Hash-Parameter der `/mifs/c/appstore/fob/`-URL

04
Übernahme – Codeausführung, Web-Shell abgelegt, Zugriff auf Gerätedaten

Betroffenheit & Fixversionen

EPMM-Zweig	Verwundbar bis	Fixversion (Ziel)
12.x.0.x	≤ 12.7.0.0	RPM 12.x.0.x
12.x.1.x	≤ 12.6.1.0	RPM 12.x.1.x
12.8.0.0	geplant Q1 2026	permanenter Fix

Ivanti liefert versionsspezifische RPM-Patches (kein Downtime) – je nach installiertem Zweig `12.x.0.x` oder `12.x.1.x`. **Wichtig:** Die RPMs überleben ein Versions-Upgrade nicht und müssen danach erneut eingespielt werden. Erst die für Q1 2026 geplante Version 12.8.0.0 enthält den dauerhaften Fix. Build-Ranges gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf gerätebezogene personenbezogene 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

29.01.2026
Ivanti veröffentlicht Advisory · CISA KEV (Frist 01.02.2026)

vor 29.01.2026
Ausnutzung als Zero-Day (begrenzte Kundenzahl) bestätigt

30.01.2026
Öffentlicher, funktionierender PoC für RCE verfügbar

Q1 2026
Version 12.8.0.0 mit permanentem Fix erwartet

Ihr Maßnahmenplan.

In dieser Reihenfolge – Exposition prüfen, patchen, Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
RPM-Patch einspielen	Exponierung reduzieren	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Installierte EPMM-Version prüfen: Alle Zweige bis einschließlich `12.7.0.0` (bzw. `12.6.1.0` im .1.x-Zweig) sind angreifbar. Prüfen, ob die EPMM-Verwaltungsoberfläche aus dem Internet erreichbar ist – das ist die Voraussetzung für die beobachtete Ausnutzung.

02 Sofort patchen

Den passenden RPM-Patch je nach Zweig einspielen (RPM `12.x.0.x` bzw. RPM `12.x.1.x`). Der Patch erfordert keine Ausfallzeit. Nach einem späteren Versions-Upgrade muss das RPM erneut aufgespielt werden, bis 12.8.0.0 (Q1 2026) den dauerhaften Fix bringt.

03 Exponierung reduzieren

Wenn kein sofortiges Patchen möglich ist: EPMM-Portal vom offenen Internet trennen bzw. hinter VPN/Access-Broker/WAF legen. CISA empfiehlt bei fehlender Mitigation, das Produkt vorübergehend außer Betrieb zu nehmen.

04 Kompromittierung ausschließen

Zugriffs- und Webserver-Logs auf verdächtige Anfragen an `/mifs/c/appstore/fob/` und `/mifs/c/aftstore/fob/` mit Bash-Mustern im Hash-Parameter durchsuchen. Auf abgelegte Web-Shells unter `/mi/tomcat/webapps/mifs/` prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Auf Vorfall vorbereiten

Bei Anzeichen einer Kompromittierung Incident-Response einleiten, Zugangsdaten/Zertifikate rotieren und den Bestand exponierter Gerätedaten für eine etwaige Meldung dokumentieren. Herstellerseitige Erkennungssignaturen einspielen, sofern verfügbar.

Kompromittierungs-Indikatoren (IoCs)

VERWUNDBARE ENDPUNKTE (GET)

`/mifs/c/appstore/fob/` (CVE-2026-1281)
`/mifs/c/aftstore/fob/` (CVE-2026-1340)

INJEKTIONS-MUSTER

Bash-Arithmetik im Hash-Parameter, z. B. `gPath[`<befehl>`]` · `sleep`-Testaufrufe

WEB-SHELLS / MARKER

`401.jsp` · `403.jsp` · `1.jsp` unter `/mi/tomcat/webapps/mifs/`

BEOBACHTETE QUELL-IPS

`23.227.199.80` · `64.7.199.177`

Zur Einordnung: Die Endpunkte sind reguläre EPMM-Aufrufe – auffällig erst durch Bash-Muster im Hash-Parameter oder ungewöhnlich lange Antwortzeiten (sleep-Tests). IPs und Dateinamen sind eine Momentaufnahme der beobachteten Kampagne und flüchtig – kein Ersatz für die Analyse Ihrer Webserver- und Zugriffslogs.

Wichtig: Ivanti bestätigt die Ausnutzung als Zero-Day vor der Veröffentlichung; ein öffentlicher PoC treibt seit dem 30.01.2026 Massen-Scans. Erfolgreiche Angriffe hinterlassen zunächst nur unauffällige Web-Requests – ohne Log-Auswertung 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: Bash-Muster in fob-Anfragen und neu abgelegte JSP-Dateien im mifs-Webroot fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, 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 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-Patch heute anordnen; falls nicht möglich, Portal vom Internet trennen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Upgrade-Pfad auf 12.8.0.0 (Q1 2026) einplanen, da RPMs Upgrades nicht überleben.

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-2026-1281 und dem EPMM-Perimeter.

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

Termin buchen

Quellen: Ivanti Security Advisory CVE-2026-1281 / CVE-2026-1340 · NVD (CVSS 3.1: 9,8) · CISA Known Exploited Vulnerabilities Catalog (hinzugefügt 29.01.2026, Frist 01.02.2026) · Rapid7 Emergent Threat Report · Palo Alto Unit 42 · watchTowr Labs · Tenable. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.