AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-6973

Ivanti EPMM: Authentifizierte Admin-RCE aktiv ausgenutzt.

Ivanti Endpoint Manager Mobile (EPMM) enthält eine Schwachstelle durch unzureichende Eingabevalidierung, über die ein bereits authentifizierter Nutzer mit Administrationsrechten aus der Ferne beliebigen Code auf dem Server ausführen kann. Die Lücke wird laut Ivanti bereits bei einer sehr begrenzten Zahl von Kunden aktiv ausgenutzt und steht seit dem 7. Mai 2026 auf der CISA-KEV-Liste. Fixversionen liegen vor; ungepatchte, exponierte Systeme sind akut gefährdet.

> **Geschäftsrisiko:** EPMM verwaltet die gesamte Mobilgeräte-Flotte samt Zertifikaten und Richtlinien. Eine Codeausführung auf diesem System bedeutet potenziell Kontrolle über alle verwalteten Endgeräte, Zugang zu Zertifikaten und einen Brückenkopf für laterale Bewegung ins Unternehmensnetz — ein Totalausfall der Mobilgeräte-Sicherheit mit direkter Melde- und Reputationsfolge.

7,2 / 10

HOCH
CVSS 3.1 BASISWERT

`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H` – Netzbasiert und mit geringer Komplexität ausnutzbar, benötigt jedoch bereits hohe Rechte (Admin); bei Erfolg volle Kompromittierung von Vertraulichkeit, Integrität und Verfügbarkeit.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
7. Mai 2026	Ivanti EPMM 12.8.0.0 und älter über die Zweige 12.6.x, 12.7.x und 12.8.x. Behoben in 12.6.1.1, 12.7.0.1 und 12.8.0.1.	Hoch — aktiv ausgenutzte KEV-Lücke mit verfügbarem Patch; kurzfristig patchen und Admin-Zugänge härten.

Das Wichtigste in 60 Sekunden.

7,2	KEV	Admin	RCE
CVSS 3.1	CISA aktiv ausgenutzt	benötigte Rechte	Auswirkung

Die Ursache: Ursache ist eine unzureichende Eingabevalidierung (CWE-20) in einer administrativen Funktion von EPMM. Ein aus der Ferne authentifizierter Nutzer mit Admin-Rolle kann manipulierte Eingaben so gestalten, dass sie in eine Codeausführung münden. Die erforderliche Admin-Authentifizierung senkt die Einstiegshürde, verhindert die Ausnutzung aber nicht — kompromittierte oder schwache Admin-Zugänge genügen.

ANGRIFFSKETTE

01
Admin-Zugang beschaffen — über gestohlene, schwache oder wiederverwendete Admin-Credentials, ggf. verkettet mit einer früheren EPMM-Lücke.

02
Eingabe manipulieren — präparierte Daten an eine administrative EPMM-Funktion senden, die die Eingabe nicht ausreichend validiert.

03
Code ausführen — beliebiger Code läuft im Kontext des EPMM-Servers (Remote Code Execution).

04
Ausweiten — Zugriff auf verwaltete Geräte, Zertifikate und Richtlinien als Brückenkopf für laterale Bewegung.

Betroffenheit & Fixversionen

EPMM-Zweig	Verwundbar bis	Fixversion (Ziel)
12.6.x und älter	< 12.6.1.1	12.6.1.1
12.7.x	12.7.0.0	12.7.0.1
12.8.x	12.8.0.0	12.8.0.1

Die Ausnutzung setzt einen authentifizierten Admin-Zugang voraus. Laut Ivanti reduziert eine bereits erfolgte Rotation der Admin-Credentials (gemäß der Januar-Empfehlung zu CVE-2026-1281/-1340) das Risiko deutlich — sie ersetzt den Patch jedoch nicht.

Regulatorischer Hinweis: NIS-2: EPMM steuert Mobilgeräte-Flotte und Zertifikate — eine erfolgreiche RCE ist ein meldepflichtiger erheblicher Sicherheitsvorfall (Frühwarnung an das BSI binnen 24 Stunden). DSGVO: Bei Zugriff auf verwaltete Geräte bzw. personenbezogene Daten greift zusätzlich die 72-Stunden-Meldepflicht nach Art. 33.

ZEITACHSE

07.05.2026
Ivanti veröffentlicht Advisory und Fixes; bestätigt begrenzte aktive Ausnutzung.

07.05.2026
CISA nimmt CVE-2026-6973 in den KEV-Katalog auf (Behörden-Frist 10.05.2026).

14.07.2026
Weiterhin aktiv relevant — ungepatchte, exponierte EPMM-Instanzen bleiben akut gefährdet.

Ihr Maßnahmenplan.

Betroffenheit prüfen, Admin-Zugänge härten, patchen und Kompromittierung ausschließen.

SOFORT	24-72 H	LAUFEND
EPMM-Version ermitteln, Admin-Zugänge und externe Exposition prüfen.	Auf Fixversion patchen, Admin-Credentials rotieren, MFA erzwingen.	EPMM als High-Value-Asset überwachen; Admin-Aktivität und ausgehende Verbindungen beobachten.

01 Betroffenheit prüfen

EPMM-Buildversion feststellen und gegen die Fix-Tabelle abgleichen. Prüfen, ob das Management-Interface aus dem Internet erreichbar ist.

```
EPMM: System Manager → Version / Software Updates
```

02 Admin-Zugänge härten

Admin-Credentials rotieren, MFA für alle Administrationskonten erzwingen und verwaiste Konten deaktivieren. Dies reduziert laut Ivanti das Ausnutzungsrisiko deutlich.

03 Patchen

Auf die jeweilige Fixversion aktualisieren: 12.6.1.1, 12.7.0.1 oder 12.8.0.1 — je nach eingesetztem Zweig.

```
12.6.x → 12.6.1.1 · 12.7.x → 12.7.0.1 · 12.8.x → 12.8.0.1
```

04 Kompromittierung ausschließen

Admin-Logins, Richtlinienänderungen, ungewöhnliche Prozess-/Shell-Ausführung und atypische ausgehende Verbindungen des EPMM-Servers prüfen. Verlässliche atomare IoCs liegen laut Ivanti nicht vor — daher verhaltensbasiert triagieren.

05 Dauerhaft überwachen

EPMM als hochwertiges Ziel in die kontinuierliche Überwachung aufnehmen und Management-Zugriff netzseitig einschränken.

⚠ **Wichtig:** Der Patch allein genügt nicht: Da die Lücke einen Admin-Zugang voraussetzt und bereits ausgenutzt wird, gehören Credential-Rotation, MFA und eine Kompromittierungsprüfung zwingend zur Behebung.

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: Auffällig im SOC wären ungewöhnliche Admin-Aktivität auf dem EPMM-Server (neue oder geänderte Richtlinien), unerwartete Prozess- oder Shell-Ausführung, atypische ausgehende Verbindungen vom Management-Host sowie Admin-Anmeldungen von untypischen Quell-IPs. fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte Endpoint Manager Mobile (EPMM) 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-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

- Sofort auf die Ivanti-Fixversion patchen und die interne SLA-Uhr für aktiv ausgenutzte KEV-Lücken starten.
- Admin-Credentials rotieren, MFA erzwingen und die Kompromittierung der letzten Wochen aktiv ausschließen.
- EPMM-Management-Zugriff aus dem Internet entfernen bzw. auf definierte Netze beschränken.

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-2026-6973 und dem Ivanti-Perimeter.

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

Termin buchen

NVD (nvd.nist.gov/vuln/detail/CVE-2026-6973); Ivanti Security Advisory (hub.ivanti.com, CVE-2026-6973 & CVE-2026-10727); CISA KEV-Katalog (Aufnahme 07.05.2026); Help Net