AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-4427

Authentifizierungs-Bypass in Ivanti EPMM (API-Komponente).

Ein nicht authentifizierter Angreifer aus dem Internet kann die API-Authentifizierung von Ivanti EPMM umgehen. Für sich genommen ist das ein Zugriff auf geschützte Ressourcen – in Kombination mit CVE-2025-4428 (Ausdrucks-Injektion) wird daraus die Ausführung von Schadcode ohne Anmeldung. Beide Lücken werden seit dem Tag der Veröffentlichung aktiv ausgenutzt.

> **Geschäftsrisiko:** vollständige Übernahme des Mobile-Device-Management-Servers – mit Potenzial für Zugriff auf verwaltete Geräte, Datenabfluss, dauerhafte Hintertüren und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

7,5 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N` – aus dem Netz, ohne Rechte, ohne Zutun – mit hoher Wirkung auf die Vertraulichkeit. NVD bewertet mit 7,5; Ivanti (CNA) mit 5,3. Erst die Verkettung mit CVE-2025-4428 (RCE) ergibt eine unauthentifizierte Remote-Code-Ausführung.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
13. Mai 2025	EPMM ≤ 11.12.0.4 · ≤ 12.3.0.1 ≤ 12.4.0.1 · ≤ 12.5.0.0 (On-Prem)	Sofort

Das Wichtigste in 60 Sekunden.

7,5 · HOCH	Auth-Bypass	Aktiv	+ CVE-2025-4428
CVSS-Schweregrad (NVD)	EPMM API-Komponente	ausgenutzt · CISA KEV · PoC öffentlich	verkettet → unauth. RCE

Die Ursache: Die API-Komponente von EPMM prüft für einen bestimmten Endpunkt die Authentifizierung nicht korrekt: durch die Reihenfolge der internen Routen erreicht eine präparierte Anfrage die Anwendungslogik, bevor die Sicherheitsfilter greifen (CWE-288, Authentifizierungs-Bypass über einen alternativen Pfad). Dahinter liegt CVE-2025-4428 – über einen nutzergesteuerten `format`-Parameter lässt sich ein Ausdruck (Expression Language) einschleusen, den der Server auswertet. Erst zusammen ergeben Bypass und Ausdrucks-Injektion die unauthentifizierte Codeausführung.

ANGRIFFSKETTE

01	02	03	04
Server exponiert – EPMM-Verwaltungsschnittstelle ist aus dem Internet erreichbar	**Auth-Bypass** – geschützten API-Endpunkt ohne gültige Anmeldung ansprechen (CVE-2025-4427)	**Ausdruck einschleusen** – über den `format`-Parameter einen EL-Ausdruck übergeben (CVE-2025-4428)	**Codeausführung** – Befehle im Kontext des EPMM-Dienstes, ohne jede Authentifizierung

Betroffenheit & Fixversionen

EPMM-Zweig	Verwundbar bis	Fixversion (Ziel)
11.12	≤ 11.12.0.4	11.12.0.5
12.3	≤ 12.3.0.1	12.3.0.2
12.4	≤ 12.4.0.1	12.4.0.2
12.5	≤ 12.5.0.0	12.5.0.1
Neurons for MDM (Cloud)	nicht betroffen	—

Betroffen ist ausschließlich das **On-Premises**-Produkt EPMM (vormals MobileIron Core). Die Cloud-Variante Ivanti Neurons for MDM ist nach Herstellerangabe nicht betroffen. Exakte Build-Ranges gegen das Hersteller-Advisory des eigenen Zweigs abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf den MDM-Server 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

13.05.2025
Ivanti veröffentlicht Advisory + Patches; erste Ausnutzung bereits bekannt

16.05.2025
Rapid7 bestätigt die Exploit-Kette in freier Wildbahn

19.05.2025
CISA nimmt beide CVEs in den KEV-Katalog auf; PoC öffentlich

Sept. 2025
CISA meldet Schadsoftware / „Malicious Listeners" auf kompromittierten Systemen (AR25-261A)

Ihr Maßnahmenplan.

In dieser Reihenfolge – exponierte Systeme zuerst, Patch vor Entwarnung.

SOFORT	FALLS NÖTIG	PARALLEL
Patch einspielen	API-Zugriff einschränken	Threat Hunting / Kompromittierung prüfen

01 Betroffenheit feststellen

Prüfen, ob ein On-Premises-EPMM (vormals MobileIron Core) betrieben wird und welche Version läuft. Angreifbar sind alle Builds ≤ 11.12.0.4, ≤ 12.3.0.1, ≤ 12.4.0.1 und ≤ 12.5.0.0. Cloud-Umgebungen (Neurons for MDM) sind nicht betroffen.

02 Patchen (vorrangig)

Auf die Fixversion des eigenen Zweigs aktualisieren (`11.12.0.5` · `12.3.0.2` · `12.4.0.2` · `12.5.0.1`). Der Patch schließt sowohl den Auth-Bypass als auch die Ausdrucks-Injektion.

03 Behelfsmaßnahme, falls kein Sofort-Patch

Bis zum Einspielen des Patches den Zugriff auf die API-Endpunkte über eine vorgelagerte WAF bzw. den integrierten Portal-ACL-Filter einschränken. Das ist ein Behelf, kein vollwertiger Ersatz für den Patch.

04 Kompromittierung ausschließen

Zugriffs- und Anwendungs-Logs auf Anfragen an den verwundbaren Endpunkt und auf auffällige `format`-Parameter durchsuchen. Auf eingeschleuste „Malicious Listeners" und unbekannte Prozesse/Dateien prüfen (CISA-Bericht AR25-261A). Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Perimeter härten

Nach Möglichkeit die EPMM-Verwaltungsschnittstelle nicht ungefiltert aus dem Internet erreichbar halten und Anmelde-/Zugriffs-Anomalien dauerhaft überwachen.

Kompromittierungs-Indikatoren (IoCs)

VERWUNDBARER ENDPUNKT (POST)

`/mifs/rs/api/v2/featureusage`

AUFFÄLLIGE MARKER

EL-Ausdrücke im `format`-Parameter (z. B. `${...}`)

ungewöhnliche Abfolge geschützter API-Aufrufe ohne gültige Session

POST-EXPLOIT

eingeschleuste „Malicious Listeners" (Java-Klassen, die Requests abfangen)

unbekannte Prozesse / Dateien – vgl. CISA AR25-261A

Zur Einordnung: Der Endpunkt ist ein regulärer EPMM-API-Aufruf – auffällig nur in Verbindung mit einem eingeschleusten Ausdruck oder Zugriffen ohne gültige Anmeldung. Die Marker stammen aus veröffentlichten Analysen und sind kein Ersatz für die Auswertung Ihrer eigenen Anwendungs- und Zugriffs-Logs.

Wichtig: Für sich genommen ist CVE-2025-4427 „nur" ein Auth-Bypass – die eigentliche Gefahr entsteht durch die Verkettung mit CVE-2025-4428 zur unauthentifizierten Codeausführung. Beide Lücken werden seit dem Tag der Veröffentlichung aktiv ausgenutzt; ein Patch allein sagt nichts darüber aus, ob ein System zuvor bereits kompromittiert wurde.

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: Zugriffe auf den verwundbaren API-Endpunkt ohne gültige Session sowie eingeschleuste Listener fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte On-Prem-EPMM-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 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

- Patch für On-Prem-EPMM sofort anordnen – die Lücken werden aktiv ausgenutzt.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung und Abschottung der MDM-Verwaltungsschnittstelle 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-2025-4427 und dem EPMM-Perimeter.

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

Termin buchen

Quellen: NVD CVE-2025-4427 · Ivanti Security Advisory EPMM (13.05.2025) · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 19.05.2025) · CISA Analysis Report AR25-261A · Rapid7 Emergent Threat Report · ProjectDiscovery Technical Analysis. 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.