AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-4428

Remote-Code-Execution in Ivanti EPMM (EL-Injection).

Zwei verkettete Schwachstellen in Ivanti EPMM erlauben es einem nicht authentifizierten Angreifer aus dem Internet, beliebigen Code auf dem Server auszuführen. Der Authentifizierungs-Umgehung (CVE-2025-4427) öffnet den ungeschützten API-Endpunkt, die EL-Injection (CVE-2025-4428) führt darüber Java-Code aus. Öffentliche Exploits existieren; die Ausnutzung läuft seit Mai 2025.

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

8,8 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz, ohne Nutzerzutun, mit vollem Verlust von Vertraulichkeit, Integrität und Verfügbarkeit. NVD wertet 8,8 (HOCH); Ivanti stuft die Einzellücke mit 7,2 ein. In Kette mit CVE-2025-4427 entfällt die Authentifizierung – der Angriff läuft unauthentifiziert.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
16. Mai 2025	EPMM ≤ 11.12.0.4 · 12.3.0.1 · 12.4.0.1 · 12.5.0.0	Sofort

Das Wichtigste in 60 Sekunden.

8,8 · HOCH
CVSS-Schweregrad (NVD)

RCE
EL-Injection · /api/v2/featureusage

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

Kette
4427 (Auth-Bypass) + 4428 (RCE)

Die Ursache: Der API-Endpunkt `/api/v2/featureusage` übergibt den vom Nutzer gelieferten `format`-Parameter ungeprüft an Springs AbstractMessageSource. Beim Aufbau von Fehlermeldungen wird der Wert als Spring-Expression-Language ausgewertet – dadurch kann ein Angreifer beliebigen Java-Code ausführen (CWE-94). Da CVE-2025-4427 diesen Endpunkt zusätzlich ohne Anmeldung erreichbar macht (fehlende Spring-Security-Regeln), ist die Kette komplett unauthentifiziert ausnutzbar.

ANGRIFFSKETTE

01
Portal exponiert – EPMM ist aus dem Internet erreichbar

02
Auth umgehen – ungeschützte Route `/api/v2/featureusage` via CVE-2025-4427 aufrufen

03
Code einschleusen – EL-Payload im `format`-Parameter (CVE-2025-4428)

04
Übernahme – Java-Code läuft, Nachladen von Sliver-Beacons beobachtet

Betroffenheit & Fixversionen

EPMM-Zweig	Verwundbar bis	Fixversion (Ziel)
11.12.0.x	≤ 11.12.0.4	11.12.0.5
12.3.0.x	≤ 12.3.0.1	12.3.0.2
12.4.0.x	≤ 12.4.0.1	12.4.0.2
12.5.0.x	12.5.0.0	12.5.0.1

Betroffen ist ausschließlich das on-premises Ivanti EPMM (vormals MobileIron Core). Ivanti Neurons for MDM (Cloud), Sentry und andere Produkte sind nach Herstellerangabe **nicht** betroffen. Fixversionen 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 (4427 + 4428)

16.05.2025
Erste aktive Ausnutzung als Zero-Day beobachtet

19.05.2025
CISA KEV · Frist für Bundesbehörden 09.06.2025

Seither
Öffentliche PoCs (watchTowr, ProjectDiscovery); fortlaufende Ausnutzung

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

Prüfen, ob ein on-premises EPMM (MobileIron Core) betrieben wird und aus dem Internet erreichbar ist. Version gegen die verwundbaren Zweige abgleichen: ≤ `11.12.0.4` · ≤ `12.3.0.1` · ≤ `12.4.0.1` · `12.5.0.0`. Cloud-basiertes Neurons for MDM ist nicht betroffen.

02 Sofort mitigieren (vor dem Patch)

Solange kein Patch möglich ist: Zugriff auf die verwundbaren API-Pfade über die eingebaute Portal-ACL bzw. eine vorgelagerte WAF einschränken – insbesondere `/api/v2/featureusage`. Ivanti verweist auf seinen ACL-Leitfaden.

```
/api/v2/featureusage → Zugriff per ACL/WAF filtern
```

03 Patchen

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 beide verketteten Lücken (4427 + 4428).

04 Kompromittierung ausschließen

Web-/API-Logs auf POST-Anfragen an `/api/v2/featureusage` bzw. `/rs/api/v2/featureusage` mit auffälligem `format`-Parameter (EL-Syntax) durchsuchen; Prozessliste und ausgehende Verbindungen auf Sliver-Beacons prüfen und die IoCs unten abgleichen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Nach Kompromittierung härten

Bei Hinweisen auf Ausnutzung: Server als kompromittiert behandeln, Zugangsdaten und Zertifikate rotieren, Persistenz und angebundene Geräte prüfen. EPMM-Zugriff dauerhaft hinter VPN/Zugriffskontrolle legen statt offen ins Internet zu stellen.

Kompromittierungs-Indikatoren (IoCs)

ANGRIFFS-ENDPUNKT (POST)

`/api/v2/featureusage`
`/rs/api/v2/featureusage`
EL-Syntax im `format`-Parameter

SLIVER-C2

`77.221.158.154`
`150.241.97.83`

BEOBACHTETE ANGREIFER-IPS

`82.132.235.212` · `37.219.84.22`
`27.25.148.183` · `47.120.74.19`

Zur Einordnung: Der Endpunkt /api/v2/featureusage ist eine reguläre EPMM-API – auffällig nur mit EL-Syntax im format-Parameter. IPs und Sliver-Infrastruktur sind eine Momentaufnahme der beobachteten Kampagne (Mai 2025) und flüchtig – kein Ersatz für die Analyse Ihrer eigenen Logs.

Wichtig: Die Auth-Umgehung (CVE-2025-4427) macht den RCE-Endpunkt ohne Anmeldung erreichbar – erfolgreiche Angriffe erzeugen keinen fehlgeschlagenen Login und lösen keinen klassischen Alarm aus. Ohne Auswertung der API-Logs 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: POST-Anfragen an /api/v2/featureusage mit EL-Payload und ausgehende Sliver-Beacons 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-premises 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

- API-Zugriff heute filtern, Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Entscheiden, ob der EPMM-Server dauerhaft hinter Zugriffskontrolle statt offen im Internet betrieben wird.

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-2025-4428 und dem EPMM-Perimeter.

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

Termin buchen

Quellen: Ivanti Security Advisory EPMM (CVE-2025-4427 / CVE-2025-4428, 13.05.2025) · NVD (CVE-2025-4428, CVSS 3.1 8,8) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 19.05.2025) · Wiz Threat Research · ProjectDiscovery / watchTowr technische Analysen. 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.