AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-29824

Unauthentifizierte SQL-Injection → RCE in Ivanti Endpoint Manager.

Ein nicht authentifizierter Angreifer im selben Netzsegment kann über eine SQL-Injection im Core-Server des Ivanti Endpoint Managers beliebigen Code ausführen – ohne Login. Da EPM eine zentrale Verwaltungsinstanz für alle verwalteten Endpunkte ist, bedeutet eine Übernahme des Servers faktisch die Kontrolle über die gesamte Client-Flotte. Die Lücke wird nachweislich aktiv ausgenutzt; ein PoC ist öffentlich.

> **Geschäftsrisiko:** Übernahme der zentralen Endpoint-Management-Infrastruktur – mit Potenzial für flächendeckende Kompromittierung der verwalteten Geräte, 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:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` – aus dem angrenzenden Netz, ohne Rechte, ohne Zutun – volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Der Hersteller (CNA) bewertet die Lücke nach CVSS 3.0 sogar mit 9,6 (kritisch).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Oktober 2024	Ivanti EPM 2022 SU5 und alle früheren Versionen	Sofort

Das Wichtigste in 60 Sekunden.

8,8 · HOCH
CVSS 3.1 · Hersteller 9,6 (3.0)

SQLi → RCE
unauthentifiziert · Core-Server

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

Adjazent
Angriff aus dem lokalen Netz

Die Ursache: Der Core-Server von Ivanti EPM übergibt eine über das Netz erreichbare Eingabe ungeprüft an eine SQL-Abfrage (CWE-89). Ein Angreifer kann dadurch eigene SQL-Befehle in die Datenbank einschleusen. Weil die Datenbank privilegiert läuft, lässt sich die Injection – etwa über `xp_cmdshell` – zur Ausführung von Betriebssystem-Befehlen auf dem Server eskalieren. Es ist keine Anmeldung erforderlich; der Angreifer muss lediglich Netzwerkzugriff auf den Core-Server im selben Segment besitzen.

ANGRIFFSKETTE

01	02	03	04
Netzzugang – Angreifer erreicht den EPM-Core-Server im selben Netzsegment (kein Login nötig)	**SQL-Injection** – manipulierte Anfrage schleust eigene SQL-Befehle in die Core-Datenbank ein	**Code-Ausführung** – über die privilegierte Datenbank (z. B. xp_cmdshell) Befehle als Dienstkonto	**Flotten-Übernahme** – der EPM-Server steuert alle verwalteten Endpunkte → flächendeckende Kontrolle

Betroffenheit & Fixversionen

EPM-Version	Verwundbar bis	Fixversion (Ziel)
2022	≤ 2022 SU5	Mai-2024-Hotpatch (Core-Server)
frühere Zweige	alle Versionen vor 2022 SU5	auf gepatchten/aktuellen Stand aktualisieren

Ivanti liefert den Fix als **Hotpatch** für den Core-Server (Austausch mehrerer DLL-Dateien, anschließend Core-Server-Neustart bzw. IISRESET). Die exakte Build-/Hotpatch-Bezeichnung des eigenen Zweigs ist vor der Umsetzung gegen das Hersteller-Advisory abzugleichen – das Advisory bündelt zehn SQL-Injection-Korrekturen im EPM-Core-Server.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die zentrale Endpoint-Management-Infrastruktur 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

Mai 2024
Ivanti veröffentlicht Advisory + Hotpatch (zehn SQLi-Fixes im Core-Server)

Juni 2024
Horizon3.ai veröffentlicht technische Analyse + PoC-Exploit

01.10.2024
Ivanti bestätigt aktive Ausnutzung ("limited number of customers")

02.10.2024
Aufnahme in CISA KEV · Frist für US-Bundesbehörden: 23.10.2024

Ihr Maßnahmenplan.

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

SOFORT	PARALLEL	DANACH
Hotpatch einspielen	Zugriff auf Core-Server einschränken	Threat Hunting / Log-Analyse

01 Betroffenheit feststellen

Inventarisieren, welche Ivanti-EPM-Core-Server im Einsatz sind und auf welchem Stand. Alle Versionen bis einschließlich 2022 SU5 sind angreifbar. Prüfen, aus welchen Netzsegmenten der Core-Server erreichbar ist – der Angriff erfolgt aus dem angrenzenden Netz, nicht zwingend aus dem Internet.

02 Hotpatch einspielen

Den von Ivanti bereitgestellten Mai-2024-Hotpatch auf dem Core-Server anwenden (Austausch der betroffenen DLL-Dateien, anschließend Core-Server-Neustart bzw. IISRESET). Exakte Hotpatch-/Build-Bezeichnung des eigenen Zweigs vorab im Hersteller-Advisory verifizieren.

03 Angriffsfläche verkleinern

Netzwerkzugriff auf den EPM-Core-Server strikt auf notwendige Verwaltungssegmente begrenzen (Segmentierung/Firewall). Da AV:A – der Angreifer muss im selben Netz stehen –, senkt eine konsequente Segmentierung das Risiko deutlich.

04 Kompromittierung ausschließen

Datenbank- und Betriebssystem-Telemetrie des Core-Servers auf Anzeichen der Ausnutzung prüfen: aktivierte/genutzte `xp_cmdshell`, unerwartete Kindprozesse des SQL-/EPM-Dienstkontos, ungewöhnliche interne Anfragen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Nachsorge

Bei Verdacht auf Kompromittierung den Vorfall dokumentieren und den Incident-Response-Prozess auslösen. Zugangsdaten/Dienstkonten des EPM-Servers rotieren und die Wirksamkeit der Segmentierung dauerhaft überwachen.

Kompromittierungs-Indikatoren (IoCs)

DATENBANK-AKTIVITÄT

Aktivierung oder Nutzung von `xp_cmdshell` auf der EPM-SQL-Instanz

PROZESS-ANOMALIEN

Unerwartete Kindprozesse (`cmd.exe`, `powershell.exe`) unter dem SQL-/EPM-Dienstkonto

ZUGRIFFSMUSTER

Auffällige, unauthentifizierte Anfragen an den Core-Server aus dem internen Netz

Zur Einordnung: Öffentlich kursiert bislang kein belastbarer Satz an Netzwerk-IoCs (IPs/Hashes) zu dieser Kampagne. Die Erkennung stützt sich auf Datenbank- und Prozess-Telemetrie des EPM-Core-Servers – kein Ersatz für die Analyse Ihrer eigenen Logs.

Wichtig: Erfolgreiche Ausnutzung hinterlässt keinen fehlgeschlagenen Login – die Injection läuft ohne Authentifizierung. Ohne gezielte Auswertung der Datenbank- und Server-Telemetrie 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: Die Nutzung von xp_cmdshell und anomale Prozesse unter dem EPM-Dienstkonto fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte Ivanti-EPM-Core-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 EPM-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

- Hotpatch für alle EPM-Core-Server sofort anordnen, Umsetzung dokumentieren.
- Netzwerkzugriff auf die EPM-Verwaltungsserver einschränken lassen (Segmentierung).
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.

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-2024-29824 und dem EPM-Perimeter.

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

Termin buchen

Quellen: Ivanti Security Advisory (Mai 2024, hub.ivanti.com) · NVD CVE-2024-29824 (CVSS 3.1: 8,8 HOCH; CNA/HackerOne CVSS 3.0: 9,6 kritisch) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 02.10.2024) · Horizon3.ai technische Analyse + PoC (Juni 2024). Angaben nach bestem Wissen zum Stand 14.07.2026; die exakte Hotpatch-/Fix-Bezeichnung des jeweiligen Zweigs ist gegen das Hersteller-Advisory abzugleichen (fix_verified=false). Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.