AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-13159

Absolute Path Traversal in Ivanti Endpoint Manager.

Ein nicht authentifizierter Angreifer aus dem Netz kann über eine absolute Pfad-Traversierung beliebige Dateien auslesen und den EPM-Server dazu bringen, sich mit seinem Maschinenkonto an einem angreiferkontrollierten Server zu authentifizieren. Der so abgegriffene Zugangs-Hash lässt sich weiterreichen (Relay) – bis hin zur Übernahme des zentralen Verwaltungsservers. Ein Trio gleichartiger Lücken (13159/13160/13161) wird seit März 2025 aktiv ausgenutzt; ein Proof-of-Concept ist öffentlich.

> **Geschäftsrisiko:** Übernahme des zentralen Endpoint-Management-Servers – und damit potenziell aller verwalteten Clients – mit Potenzial für Datenabfluss, Ransomware-Ausbreitung 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, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Ivanti bewertet die Lücke mit 9,8 (kritisch); das NIST-NVD stuft sie – bei reinem Informationsabfluss – mit 7,5 ein.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
März 2025	EPM 2024 & EPM 2022 SU6 bis November-2024-Update	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (Ivanti)

Path Traversal
unauth. · CWE-36

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

EPM 2024 & 2022 SU6
zentraler Management-Server

Die Ursache: Verwundbare EPM-Versionen prüfen einen vom Angreifer übergebenen Dateipfad nicht ausreichend gegen eine absolute Pfad-Traversierung ab (CWE-36). Ein nicht authentifizierter Angreifer kann so beliebige Dateien außerhalb des vorgesehenen Verzeichnisses auslesen. Gibt er einen **UNC-Pfad** auf einen eigenen Server an, verbindet sich der EPM-Server mit dem Maschinenkonto dorthin – und gibt dabei seinen NTLM-Authentifizierungs-Hash preis, der sich per Relay gegen andere Dienste weiterverwenden lässt.

ANGRIFFSKETTE

01 **EPM erreichbar** – der Endpoint-Manager-Server ist im Netz ansprechbar

02 **Pfad manipulieren** – absolute Traversierung auf eine beliebige Datei oder einen UNC-Pfad

03 **Credential leaken** – der Server authentifiziert sich mit seinem Maschinenkonto beim Angreifer

04 **Relay & Übernahme** – abgegriffener Hash wird weitergereicht bis zur Server-Kontrolle

Betroffenheit & Fixversionen

EPM-Zweig	Verwundbar bis	Fixversion (Ziel)
EPM 2024	≤ November-2024 Security Update	2024 January-2025 Security Update
EPM 2022 SU6	≤ November-2024 Security Update	2022 SU6 January-2025 Security Update
Cloud-Services	nicht betroffen	—

Betroffen sind on-premises EPM 2024 und EPM 2022 SU6 jeweils bis einschließlich des November-2024-Security-Updates. Die Lücke wurde im **January-2025 Security Update** beider Zweige behoben – exakten Update-Stand gegen das Hersteller-Advisory abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff oder Datenabfluss über den EPM-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

Okt. 2023
Schwachstelle an Ivanti gemeldet (Horizon3.ai)

13.01.2025
Ivanti veröffentlicht Advisory & Fixes

Feb. 2025
Öffentlicher Proof-of-Concept-Exploit

10.03.2025
CISA KEV – Nachweis aktiver Ausnutzung

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Betroffenheit feststellen	January-2025-Update einspielen	Threat Hunting / Log-Abgleich

01 Betroffenheit feststellen

Prüfen, ob Ivanti Endpoint Manager 2024 oder 2022 SU6 im Einsatz ist und welcher Security-Update-Stand installiert ist. Alles bis einschließlich November-2024-Update ist angreifbar. Insbesondere aus dem Netz erreichbare EPM-Server priorisieren.

02 Netz-Exposition begrenzen

Den EPM-Server bis zum Patch nicht aus nicht vertrauenswürdigen Netzen erreichbar halten; ausgehende SMB-/NTLM-Verbindungen vom Server auf das Notwendige beschränken, um Credential-Leak per Relay zu erschweren.

03 Patchen

Das `January-2025 Security Update` für den jeweiligen Zweig einspielen (EPM 2024 bzw. EPM 2022 SU6). Es behebt CVE-2024-13159 gemeinsam mit den verwandten Lücken 13160, 13161 und 10811.

04 Kompromittierung ausschließen

Authentifizierungs- und Netzwerk-Logs auf ausgehende Anmeldungen des EPM-Maschinenkontos an unerwarteten Zielen sowie auf ungewöhnliche Zugriffe auf EPM-Endpunkte durchsuchen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Perimeter absichern

Herstellerseitige bzw. IPS-Signaturen für diese Schwachstellen einspielen, sofern verfügbar, und exponierte EPM-Instanzen dauerhaft überwachen. Verwandte, gleichartige Lücken desselben Advisories mit behandeln.

Kompromittierungs-Indikatoren (IoCs)

KERNINDIKATOR	LOG-AUFFÄLLIGKEITEN	FOLGEAKTIVITÄT
Ausgehende `SMB/NTLM`-Authentifizierung des EPM-Maschinenkontos an unerwartete/externe Ziele	Unauthentifizierte Zugriffe auf EPM-Web-/API-Endpunkte mit auffälligen absoluten oder `UNC`-Pfaden	Relay-Anmeldungen des EPM-Kontos an Datei-/AD-Diensten · unerwartete Rechte-Ausweitung am Server

Zur Einordnung: Für diese Kampagne sind keine belastbaren, stabilen Netz-IoCs (feste IPs/Hostnamen) öffentlich – die Ausnutzung nutzt legitime Authentifizierungs-Mechanismen. Entscheidend ist die Auswertung Ihrer eigenen Authentifizierungs- und Netzwerk-Logs rund um den EPM-Server.

Wichtig: Der Angriff missbraucht reguläre Windows-Authentifizierung: Der geleakte Maschinenkonto-Hash erscheint zunächst als normale Anmeldung. Ohne gezielte Auswertung ausgehender Server-Authentifizierungen 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 ausgehende Maschinenkonto-Authentifizierung des EPM-Servers und anomale Zugriffe auf EPM-Endpunkte 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-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

- January-2025-Update umgehend einplanen und exponierte EPM-Server zuerst patchen.
- Prüfen lassen, ob bereits ein Zugriff oder Credential-Leak erfolgt ist – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung des zentralen Management-Servers 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-2024-13159 und dem EPM-Perimeter.

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

Termin buchen

Quellen: Ivanti Security Advisory EPM January 2025 (EPM 2024 / EPM 2022 SU6) · NIST NVD CVE-2024-13159 · CISA Known Exploited Vulnerabilities Catalog (hinzugefügt 10.03.2025) · Horizon3.ai. Angaben nach bestem Wissen zum Stand 14.07.2026; Update-Stände gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Ivanti bewertet die Lücke mit CVSS 9,8 (kritisch), das NIST-NVD mit 7,5. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.