AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-13161

Absolute Path Traversal in Ivanti Endpoint Manager.

Ein nicht authentifizierter Angreifer aus dem Netz kann über einen manipulierten Datei-Pfad den EPM-Server dazu zwingen, sich bei einem angreiferkontrollierten Server anzumelden – und die dabei preisgegebenen Maschinenkonto-Zugangsdaten weiterreichen (Relay). In der Praxis führt das bis zur vollständigen Übernahme des EPM. Die Lücke ist Teil eines Trios (mit CVE-2024-13159 und CVE-2024-13160), steht seit dem 10. März 2025 im CISA-KEV-Katalog, und öffentlicher PoC-Code existiert.

> **Geschäftsrisiko:** unbefugter Zugriff bis hin zur Übernahme der zentralen Endpoint-Management-Plattform – mit Potenzial für flächige Kompromittierung verwalteter Endpunkte, Datenabfluss 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 hoher Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Herstellerbewertung von Ivanti; NIST/NVD stuft dieselbe Lücke mit 7,5 (HOCH) ein, da die Erstwirkung ein Informationsabfluss ist.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Aufnahme in CISA KEV: 10. März 2025	EPM 2024 & EPM 2022 SU6 (vor Jan-2025-Update)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (Hersteller)

Path Traversal
unauth. · Credential-Coercion

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

Trio
mit CVE-2024-13159 / -13160

Die Ursache: Betroffene EPM-Funktionen berechnen Datei-Hashes und lesen dafür Dateien in bestimmten Verzeichnissen – die dafür übergebenen Pfadangaben werden jedoch nicht validiert (CWE-36, absolute Path Traversal). Ein Angreifer kann so einen Pfad übergeben, der auf einen entfernten **UNC-Pfad** (`\\angreifer\share`) zeigt. Der EPM-Core-Server verbindet sich daraufhin selbst zu diesem Server und gibt dabei die Zugangsdaten seines Maschinenkontos preis. Diese lassen sich per NTLM-Relay an das LDAP weiterreichen, um ein Maschinenkonto anzulegen und den EPM zu kompromittieren.

ANGRIFFSKETTE

01	02	03	04
Dienst erreichbar – der EPM-Core-Server-Webdienst ist ohne Authentifizierung erreichbar	**Pfad manipulieren** – Hash-Funktion mit einem UNC-Pfad auf einen angreiferkontrollierten Server aufrufen	**Zwangs-Anmeldung** – EPM-Server authentifiziert sich am fremden Server und leakt Maschinenkonto-Credentials (NTLM)	**Relay & Übernahme** – Credentials an LDAP weiterreichen, Maschinenkonto anlegen, EPM übernehmen

Betroffenheit & Fixversionen

EPM-Version	Verwundbar bis	Fixversion (Ziel)
EPM 2024	vor Jan-2025-Update	2024 January-2025 Security Update
EPM 2022 SU6	vor Jan-2025-Update	2022 SU6 January-2025 Security Update
EPM 2022 SU5 & älter	nicht mehr direkt gepatcht	zuerst auf 2022 SU6 heben, dann Jan-2025-Update

Fixes stehen nur für die unterstützten Zweige EPM 2024 und EPM 2022 SU6 bereit. Ältere 2022-Servicepacks (SU1–SU5) müssen zunächst auf SU6 angehoben werden. Die exakte Build-/Update-Bezeichnung gegen das Hersteller-Advisory des eigenen Zweigs abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff oder Informationsabfluss 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

Jan. 2025
Ivanti veröffentlicht Advisory + January-2025 Security Update

24.02.2025
Horizon3.ai veröffentlicht PoC-Exploit-Code

10.03.2025
Aufnahme in CISA KEV · BOD-22-01-Frist 31.03.2025

Seither
Als aktiv ausgenutzt geführt

Ihr Maßnahmenplan.

In dieser Reihenfolge – Betroffenheit klären, patchen, dann Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Betroffenheit & Exposition prüfen	January-2025-Update einspielen	Threat Hunting / IoC-Abgleich

01 Betroffenheit feststellen

Version und Update-Stand des EPM-Core-Servers prüfen: Läuft EPM 2024 oder EPM 2022 SU6 ohne das January-2025 Security Update? Ältere 2022-Servicepacks (SU1–SU5) gelten ebenfalls als angreifbar und müssen zunächst auf SU6 gehoben werden.

02 Exposition eingrenzen (vor dem Patch)

Prüfen, ob der EPM-Core-Server-Webdienst über das interne Netz hinaus erreichbar ist, und den Zugriff auf das Nötige beschränken. Ausgehende SMB-/UNC-Verbindungen (TCP 445) vom EPM-Server nach außen an der Firewall unterbinden – das erschwert die Zwangs-Authentifizierung.

03 Patchen

Auf das `January-2025 Security Update` des eigenen Zweigs aktualisieren (EPM 2024 bzw. EPM 2022 SU6). Es adressiert das gesamte Trio CVE-2024-13159 / -13160 / -13161.

04 Kompromittierung ausschließen

Auf dem EPM-Server nach unerwarteten ausgehenden SMB-Verbindungen suchen und im Active Directory nach neu angelegten Maschinenkonten fahnden. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Credential-Relay-Angriff.

05 Trio gesamthaft behandeln

CVE-2024-13161 tritt gemeinsam mit CVE-2024-13159 und CVE-2024-13160 auf; alle drei sind Path-Traversal-Lücken im selben EPM und stehen im CISA-KEV-Katalog. Betroffenheits- und Patch-Status für alle drei gemeinsam dokumentieren.

Kompromittierungs-Indikatoren (IoCs)

NETZ-AUFFÄLLIGKEITEN

Ausgehende SMB-/UNC-Verbindungen `(TCP 445)` vom EPM-Core-Server zu unerwarteten oder externen Zielen

ACTIVE DIRECTORY

Neu angelegte, unerklärte `Maschinen-/Computerkonten` · NTLM-Anmeldungen des EPM-Maschinenkontos an fremden Zielen

ANWENDUNGSSEITIG

Aufrufe der EPM-Hash-/Datei-Funktionen mit Pfadparametern in UNC-Form `(\\host\share)`

Zur Einordnung: Es sind keine belastbaren, öffentlich bestätigten Angreifer-IPs oder festen Datei-IoCs zu dieser Kampagne veröffentlicht. Die genannten Indikatoren sind verhaltensbasiert – kein Ersatz für die Auswertung Ihrer EPM-Server- und Active-Directory-Protokolle.

Wichtig: Der Angriff läuft über den EPM-Server selbst: Er wird gezwungen, sich am angreiferkontrollierten Server anzumelden. Erfolgreiche Ausnutzung hinterlässt kaum Alarme – auffällig ist vor allem die ausgehende SMB-Verbindung des Servers und ein neues Maschinenkonto im AD.

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 SMB-Zwangsanmeldung des EPM-Servers und die Anlage eines neuen Maschinenkontos 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 Ivanti 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 auf allen EPM-Servern kurzfristig einplanen – das Trio 13159/13160/13161 gemeinsam schließen.
- Prüfen lassen, ob bereits ein Credential-Relay erfolgt ist – dokumentiert für eine etwaige Meldung.
- Erreichbarkeit des EPM-Core-Servers und ausgehende SMB-Verbindungen dauerhaft einschränken und überwachen.

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-2024-13161 und dem Ivanti 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) · NVD CVE-2024-13161 (NIST 3.1 = 7,5; CNA/Ivanti 3.1 = 9,8; CWE-36) · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 10.03.2025, Frist 31.03.2025, Ransomware-Nutzung: unbekannt) · Horizon3.ai PoC-Analyse. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Bezeichnungen gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.