AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-13160

Absolute Path Traversal in Ivanti Endpoint Manager.

Ein nicht authentifizierter Angreifer aus dem Netz kann über einen absoluten Dateipfad beliebige Dateien vom EPM-Server auslesen. In der veröffentlichten Angriffskette wird die Lücke genutzt, um das EPM-Maschinenkonto zu einer Authentifizierung zu zwingen und diese weiterzuleiten (Relay) – bis hin zur Ausweitung der Rechte im Active Directory. Die Schwachstelle ist Teil eines Trios (CVE-2024-13159 / -13160 / -13161) und wird aktiv ausgenutzt.

Geschäftsrisiko: unbefugter Zugriff auf zentrale Verwaltungsserver und Domänen-Anmeldeinformationen – mit Potenzial für flächige Kompromittierung, 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 Potenzial zur vollständigen Kompromittierung. Ivanti bewertet die Lücke als Hersteller mit 9,8 (kritisch); das NVD führt einen abweichenden, niedrigeren Basiswert von 7,5 (nur Vertraulichkeit).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
März 2025	EPM 2024 & EPM 2022 SU6 vor dem Januar-2025-Update	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (Ivanti)

Path Traversal
unauth. Dateizugriff aus dem Netz

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

Teil eines Trios
mit CVE-2024-13159 / -13161

Die Ursache: Ivanti EPM prüft in den verwundbaren Ständen einen übergebenen Dateipfad unzureichend. Ein Angreifer kann einen **absoluten Pfad** übermitteln und so beliebige Dateien vom EPM-Server auslesen – ohne Anmeldung. In der von Horizon3.ai veröffentlichten Angriffskette wird dies genutzt, um das **EPM-Maschinenkonto** zu einer NTLM-Authentifizierung zu bewegen und diese auf andere Dienste weiterzuleiten (Relay) – der Weg zur Rechteausweitung bis hin zur Domänenübernahme.

ANGRIFFSKETTE

01
EPM erreichbar – Verwaltungsserver ist aus dem Netz ansprechbar

02
Traversal-Request – absoluter Dateipfad an einen EPM-Web-Endpunkt

03
Coercion – EPM-Maschinenkonto wird zur Authentifizierung gezwungen

04
Relay & Ausweitung – Weiterleitung der Anmeldung bis zur Domänenübernahme

Betroffenheit & Fixversionen

EPM-Version	Verwundbar bis	Fixversion (Ziel)
EPM 2024	vor dem Januar-2025 Security Update	2024 Januar-2025 Security Update
EPM 2022	SU1–SU5 & SU6 vor dem Januar-2025 Security Update	2022 SU6 Januar-2025 Security Update

Betroffen sind EPM 2024 und EPM 2022 SU6 vor dem jeweiligen Januar-2025 Security Update. Exakte Build-Stände gegen das Ivanti-Advisory des eigenen Zweigs abgleichen; EPM 2022 wird nur noch über SU6 versorgt. Ältere, abgekündigte EPM-Stände erhalten keinen Fix und sollten migriert werden.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff – insbesondere auf Anmeldeinformationen oder personenbezogene Daten – 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

13.01.2025
Ivanti veröffentlicht Advisory und Patches

Feb. 2025
Horizon3.ai veröffentlicht technische Analyse / PoC

10.03.2025
CISA nimmt den CVE in den KEV-Katalog auf – aktive Ausnutzung

31.03.2025
CISA-Frist zur Behebung für US-Behörden

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Exposure prüfen & einschränken	Januar-2025-Update einspielen	Threat Hunting / Credential-Rotation

01 Betroffenheit & Exposure feststellen

EPM-Version und Patch-Stand ermitteln (EPM 2024 bzw. 2022 SU6). Prüfen, ob der EPM-Server aus dem Internet oder untypischen Netzsegmenten erreichbar ist – die Angriffsfläche soweit möglich auf das Verwaltungsnetz beschränken.

02 Patchen

Das jeweilige **Januar-2025 Security Update** einspielen (EPM 2024 Januar-2025 SU bzw. EPM 2022 SU6 Januar-2025 SU). Kein belastbarer Workaround bekannt – der Patch ist der einzige verlässliche Schutz.

03 Kompromittierung ausschließen

Zugriffs- und Authentifizierungslogs auf Path-Traversal-Anfragen an EPM-Endpunkte und auf anomale NTLM-/SMB-Authentifizierungen des EPM-Maschinenkontos durchsuchen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

04 Anmeldeinformationen rotieren

Bei Verdacht auf Ausnutzung das EPM-Maschinenkonto sowie betroffene Dienst-/Domänenkonten zurücksetzen. Relay-Angriffe zielen auf Anmeldeinformationen – ein reiner Patch stellt keine bereits abgeflossenen Credentials wieder her.

05 Trio gesamthaft behandeln

Die Schwachstelle gehört zu einem Trio (CVE-2024-13159 / -13160 / -13161), das dasselbe Update schließt. Alle drei gemeinsam abarbeiten und die Fixstände gegen das Ivanti-Advisory bestätigen.

Kompromittierungs-Indikatoren (IoCs)

TRAVERSAL-MUSTER

HTTP-Anfragen an EPM-Web-Endpunkte mit absoluten Pfaden bzw. `\..\`-Sequenzen aus untypischen Quellen

CREDENTIAL-COERCION

unerwartete NTLM-/SMB-Authentifizierung vom EPM-`Maschinenkonto` an fremde Hosts

EXPOSURE

Zugriffe auf den EPM-Server aus dem Internet oder aus fremden Netzsegmenten

Zur Einordnung: Für diese Schwachstelle liegt kein stabiler, öffentlich verifizierter Satz an Netzwerk-IoCs (feste IPs/Hashes) vor. Die Erkennung ist verhaltensbasiert: Traversal-Muster in den EPM-Zugriffslogs und anomale Authentifizierung des EPM-Maschinenkontos sind die belastbaren Signale – kein Ersatz für die Analyse Ihrer eigenen Logs.

Wichtig: Erfolgreiche Angriffe hinterlassen zunächst nur reguläre Datei- bzw. Authentifizierungsvorgänge des EPM-Kontos – ohne Alarm. Ohne Auswertung der EPM-Zugriffs- und AD-Authentifizierungslogs bleibt ein bereits erfolgtes Credential-Relay 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: Path-Traversal-Zugriffe auf EPM und anomale Authentifizierung des EPM-Maschinenkontos fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Netz erreichbare, ungepatchte 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 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

- Januar-2025 Security Update kurzfristig einplanen und die Erreichbarkeit des EPM-Servers einschränken.
- Prüfen lassen, ob bereits ein Zugriff oder Credential-Relay erfolgt ist – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung der Verwaltungsserver und des Perimeters 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-2024-13160 und dem Ivanti EPM-Perimeter.

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

Termin buchen

Quellen: Ivanti Security Advisory EPM (Januar 2025) für EPM 2024 und EPM 2022 SU6 · National Vulnerability Database (NVD) CVE-2024-13160 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 10.03.2025) · Horizon3.ai Analyse (Zach Hanley). Hinweis: Ivanti (CNA) bewertet die Lücke mit CVSS 9,8; das NVD führt einen abweichenden Basiswert von 7,5. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixstände gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.