AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-1603

Authentifizierungs-Bypass in Ivanti Endpoint Manager.

Ein nicht authentifizierter Angreifer aus dem Netz kann über einen undokumentierten Login-Parameter die Anmeldung des Endpoint Managers umgehen und gespeicherte Zugangsdaten auslesen – bis hin zu Passwort-Hashes von Domänen-Administratoren und Dienstkonten aus dem EPM-Credential-Vault. Der technische Mechanismus ist seit Februar 2026 öffentlich, die Lücke steht seit dem 9. März 2026 im CISA-KEV-Katalog als aktiv ausgenutzt.

Geschäftsrisiko: Diebstahl privilegierter Anmeldedaten aus dem zentralen Management-Server – mit Potenzial für Übernahme der Domäne, flächige Kompromittierung verwalteter Endpunkte und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

8,6 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N` – aus dem Netz, ohne Rechte, ohne Zutun – hohe Vertraulichkeitswirkung mit Ausbruch über die verwundbare Komponente hinaus (Scope: Changed). Herstellerwert von Ivanti; das NIST NVD bewertet dieselbe Lücke mit 7,5 (Scope: Unchanged).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
9. März 2026 (CISA KEV)	EPM 2024 – alle Stände vor 2024 SU5	Sofort

Das Wichtigste in 60 Sekunden.

8,6 · HOCH
CVSS-Schweregrad (Ivanti)

Auth-Bypass
logintype=64 · Credential Vault

Aktiv
ausgenutzt · CISA KEV

Fix: 2024 SU5
Ivanti Feb-2026-Update

Die Ursache: Der Anmelde-Endpunkt des Endpoint Managers akzeptiert einen undokumentierten Parameter `logintype` mit dem Wert 64. Dieser aktiviert einen alternativen, fest verdrahteten Authentifizierungspfad, der die reguläre Prüfung von Anmeldedaten umgeht (CWE-288 · CWE-306). Wer den Parameter kennt, erhält ohne gültige Zugangsdaten privilegierten Zugriff und kann gespeicherte Credentials des EPM auslesen.

ANGRIFFSKETTE

01
Server exponiert – EPM-Managementdienst über HTTP/HTTPS (Port 80/443) erreichbar

02
Bypass auslösen – POST an den Auth-Endpunkt mit `logintype=64`

03
Zugriff – privilegierter Zugang ohne gültige Anmeldedaten

04
Credentials abgreifen – gespeicherte Zugangsdaten aus dem EPM-Vault, u. a. Domänen-Admin-Hashes

Betroffenheit & Fixversionen

EPM-Version	Verwundbar bis	Fixversion (Ziel)
EPM 2024	< 2024 SU5 (inkl. SU1–SU4 & Security Releases)	2024 SU5
Ältere Zweige (EPM 2022 & früher)	End-of-Life – kein Sicherheitsupdate	Migration auf 2024 SU5

Fix ausschließlich in **EPM 2024 SU5** (Ivanti-Update Februar 2026). Alle Stände davor sind verwundbar. Ältere, nicht mehr unterstützte Zweige erhalten kein Update – hier ist eine Migration erforderlich. Exakten Patch-Stand gegen das Ivanti-Advisory abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf gespeicherte Zugangsdaten 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

10.02.2026
Ivanti veröffentlicht Advisory (EPM Februar 2026, Fix in 2024 SU5)

13.02.2026
WatchTowr legt den logintype=64-Bypass öffentlich offen

09.03.2026
CISA KEV: aktiv ausgenutzt · Behördenfrist 23.03.2026

Seither
Fortlaufende Ausnutzung exponierter, ungepatchter Server

Ihr Maßnahmenplan.

In dieser Reihenfolge – Erreichbarkeit einschränken vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Zugriff einschränken	Auf 2024 SU5 patchen	Credentials rotieren & Threat Hunting

01 Betroffenheit feststellen

EPM-Version ermitteln. Jeder Stand von EPM 2024 vor `2024 SU5` sowie ältere, nicht mehr unterstützte Zweige sind verwundbar. Prüfen, ob der Managementdienst aus nicht vertrauenswürdigen Netzen erreichbar ist.

02 Sofort Erreichbarkeit einschränken (vor dem Patch)

Externen Zugriff auf die EPM-Ports 80/443 blockieren und Zugriff per IP-Allowlist auf vertrauenswürdige Administrations-Hosts begrenzen – von CISA als Behelf bis zum Patch benannt.

03 Patchen

Auf `EPM 2024 SU5` aktualisieren (Ivanti-Update Februar 2026) – die einzige Version, in der die Lücke geschlossen ist. Ältere Zweige erfordern eine Migration auf 2024 SU5.

04 Kompromittierung ausschließen & Credentials rotieren

Da ein erfolgreicher Zugriff gespeicherte Zugangsdaten preisgibt: im EPM-Vault hinterlegte Konten – insbesondere Domänen-Admin- und Dienstkonten – als potenziell kompromittiert behandeln und Passwörter rotieren. Ein Patch schließt die Lücke, nicht einen bereits erfolgten Abfluss.

05 Überwachen

Web-/WAF-Logs des EPM auf Anfragen mit dem Parameter `logintype=64` am Auth-Endpunkt durchsuchen sowie auf unerwartete Administrator-/Kontenanlagen und anomale ausgehende Verbindungen des EPM-Servers.

Kompromittierungs-Indikatoren (IoCs)

ANGRIFFSMUSTER (POST)

Auth-Endpunkt mit Parameter `logintype=64`
z. B. `/RemoteControlAuth/api/Auth`

AUFFÄLLIGE AKTIVITÄT

unerwartete Administrator-/Kontenanlagen
Zugriffe auf den EPM-Credential-Vault ohne gültige Anmeldung

NETZ

unautorisierte Zugriffe auf EPM-Dienste
anomale ausgehende Verbindungen des EPM-Servers

Zur Einordnung: Ivanti hat keine belastbaren Netz-IoCs (Angreifer-IPs) veröffentlicht. Ohne WAF-/Reverse-Proxy-Logs, die den Parameter logintype erfassen, ist eine Kompromittierung schwer nachzuweisen. Die genannten Marker sind Erkennungshinweise, kein abschließender IoC-Satz – maßgeblich ist die Analyse Ihrer eigenen Logs.

Wichtig: Ein erfolgreicher Bypass hinterlässt in Standardprotokollen kaum Spuren und liefert dem Angreifer sofort gespeicherte Zugangsdaten. Ohne Auswertung der Auth-/WAF-Logs und ohne Rotation der im Vault hinterlegten Konten 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: Anfragen mit logintype=64 am Auth-Endpunkt und unerwartete privilegierte Aktionen im EPM fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte Ivanti-EPM-Managementserver 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

- Externen Zugriff auf den EPM heute einschränken, Patch auf 2024 SU5 innerhalb der Behördenfrist (23.03.2026) einplanen.
- Im EPM-Vault hinterlegte privilegierte Konten rotieren und prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung des Perimeters und der Management-Server 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-2026-1603 und dem Ivanti EPM-Perimeter.

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

Termin buchen

Quellen: Ivanti Security Advisory EPM February 2026 (Fix in 2024 SU5) · NIST NVD CVE-2026-1603 · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 09.03.2026, Frist 23.03.2026) · WatchTowr Labs / Beazley Security / Horizon3.ai (technische Analyse, logintype=64). Angaben nach bestem Wissen zum Stand 14.07.2026; Patch-Stand und Versionsangaben gegen das Ivanti-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.