THREAT INTELLIGENCE BRIEFING

CVE-2026-121653

Codeausführung ohne Anmeldung in Ivanti Endpoint Manager.

Ein nicht authentifizierter Angreifer kann über eine SQL-Injection im Core-Server von Ivanti Endpoint Manager eigenen Code ausführen. Der Core-Server verteilt Software und Einstellungen auf alle verwalteten Endgeräte – wer ihn übernimmt, hat einen zentralen Hebel ins Unternehmensnetz. Ivanti hat die Lücke am 10.11.2026 mit Version 2024 SU8 geschlossen; eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** Übernahme der zentralen Endgeräteverwaltung und damit Zugriff auf alle verwalteten Clients und Server – mit Potenzial für Ransomware-Verteilung, 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 voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Von Ivanti als CNA vergeben; NVD-Status „Received“, noch keine eigene NIST-Bewertung.

AUSNUTZUNG	BETROFFEN	HANDLUNGSBEDARF
Nicht bekannt (Stand 10.11.2026)	EPM 2024 SU7 und älter	Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

SQL-Injection
führt zu Codeausführung ohne Anmeldung

Nicht bekannt
Ausnutzung · nicht in CISA KEV · kein PoC öffentlich

2024 SU8
Fixversion seit 10.11.2026

Die Ursache: Der Core-Server von Ivanti Endpoint Manager verarbeitet Eingaben aus dem Netz, ohne Sonderzeichen in SQL-Befehlen ausreichend zu neutralisieren (CWE-89, SQL-Injection). Ein Angreifer ohne Anmeldung kann dadurch eigene Datenbankbefehle einschleusen und laut Ivanti bis zur Ausführung von Code auf dem Server gelangen. Technische Details zum betroffenen Endpunkt hat Ivanti nicht veröffentlicht.

ANGRIFFSKETTE

01	02	03	04
Core erreichbar – EPM-Core-Server ist aus dem Netz ansprechbar	**SQL einschleusen** – präparierte Anfrage ohne Anmeldung senden	**Code ausführen** – Kontrolle über den Core-Server	**Ausbreitung** – Verteilung über die verwalteten Endgeräte möglich

Betroffenheit & Fixversionen

EPM-Version	Verwundbar bis	Fixversion (Ziel)
EPM 2024	bis 2024 SU7	2024 SU8
Ältere Releases	vor 2024 SU8	Upgrade auf 2024 SU8

Betroffen ist laut Ivanti (CVE-Eintrag, Ivanti als CNA) jede Endpoint-Manager-Version **vor 2024 SU8**, konkret die Core-Komponente. Ivanti nennt keinen Workaround. Am selben Tag hat Ivanti mit SU8 eine weitere EPM-Lücke geschlossen (CVE-2026-18128, CVSS 6,8, Klartext-Übertragung beim Agent).

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die Endgeräteverwaltung 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

03.11.2026
CVE-Nummer reserviert

10.11.2026
Ivanti-Advisory · Fix 2024 SU8

10.11.2026
Keine Ausnutzung bekannt

Stand heute
Nicht in CISA KEV · kein PoC

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Erreichbarkeit einschränken	2024 SU8 einspielen	Core-Server prüfen

01 Betroffenheit feststellen

Version aller EPM-Core-Server erfassen. Alles vor 2024 SU8 ist betroffen. Prüfen, aus welchen Netzen der Core erreichbar ist – insbesondere, ob er aus dem Internet oder aus Gast- und Partnernetzen angesprochen werden kann.

02 Exposition reduzieren (vor dem Patch)

Ivanti nennt keinen Workaround. Bis zum Update den Zugriff auf den Core-Server per Firewall auf die Netze beschränken, aus denen Agents und Administratoren tatsächlich kommen. Das ersetzt den Patch nicht.

03 Patchen

Auf 2024 SU8 aktualisieren. Damit ist auch die zweite November-Lücke (CVE-2026-18128) geschlossen.

04 Kompromittierung ausschließen

Datenbank- und Webserver-Logs des Core auf ungewöhnliche Anfragen, neue Administratorkonten, unbekannte Prozesse und neu angelegte Softwareverteilungen oder Skripte prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Stand 10.11.2026 keine Ausnutzung bekannt, kein öffentlicher PoC

AUSWERTUNGSQUELLEN

IIS-/Webserver-Logs des Core
SQL-Server-Logs der EPM-Datenbank

AUFFÄLLIGE MUSTER

unerwartete Prozesse unter dem Core-Dienst
neue Verteilaufgaben / Skripte
neue Konsolen-Administratoren

Zur Einordnung: Es liegen keine CVE-spezifischen Indikatoren vor. Die genannten Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

Wichtig: Wer den Core-Server kontrolliert, kann über die reguläre Softwareverteilung Code auf alle verwalteten Geräte bringen – das sieht aus wie normaler Betrieb. Ohne Überwachung des Core fällt ein Missbrauch erst spät auf.

Bildmotive: KI-generierte Symbolbilder

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: Ein unerwarteter Prozess oder eine neue Verteilaufgabe auf dem EPM-Core fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte 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

- Update auf 2024 SU8 priorisiert anordnen.
- Prüfen lassen, aus welchen Netzen der Core-Server erreichbar ist.
- Über eine dauerhafte Überwachung zentraler Verwaltungssysteme 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-2026-121653 und dem Ivanti EPM-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: CVE-Eintrag CVE-2026-121653 (Ivanti als CNA, CVSS 3.1 9,8, CWE-89, Fix 2024 SU8) · NVD (Status „Received“) · Ivanti Security Advisory EPM November 2026 · CISA KEV (Stand 10.11.2026: nicht gelistet) · ergänzend SecurityOnline. Stand 10.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.