AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-103406

Root-Befehlsausführung in Juniper Session Smart Conductor.

Ein Angreifer ohne Anmeldung kann auf dem Juniper Session Smart Conductor beliebige Befehle mit Root-Rechten ausführen – über eine präparierte Salt-Minion-ID bei der Schlüsselverwaltung. Der Conductor steuert alle angebundenen Session Smart Router; Juniper bestätigt mindestens einen Fall von Ausnutzung, CISA führt die Lücke seit dem 25.11.2026 als aktiv ausgenutzt.

Geschäftsrisiko: vollständige Übernahme der zentralen Steuerung des SD-WAN – mit Zugriff auf Konfiguration und angebundene Standorte, möglicher Betriebsunterbrechung und einem 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 Anmeldung, ohne Zutun eines Nutzers, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Wert von Juniper (JSA112183), von NVD übernommen.

AUSGENUTZT SEIT
spätestens November 2026

BETROFFEN
Session Smart Conductor vor 7.0.5 · 7.1.x vor 7.1.7 · 7.2.x vor 7.2.3

HANDLUNGSBEDARF
Sofort

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS 3.1 Basiswert (Juniper)

Root-RCE
ohne Anmeldung · AutomatedProvisioner

Aktiv
ausgenutzt · CISA KEV · Frist 28.11.2026

Kein Workaround
nur Update auf 7.0.5 / 7.1.7 / 7.2.3

Die Ursache: Der Dienst **AutomatedProvisioner** des Session Smart Conductor verarbeitet bei der Schlüsselverwaltung die **Minion-ID**, mit der sich ein per Salt verwalteter Knoten meldet. Sonderzeichen in diesem Wert werden nicht ausreichend neutralisiert und landen in einem Betriebssystem-Befehl (CWE-78). Ein Angreifer, der den Dienst über das Netz erreicht, kann so ohne Anmeldung eigene Befehle als Root einschleusen.

ANGRIFFSKETTE

01 **Conductor erreichbar** – Provisionierungs-Dienst ist aus dem Netz ansprechbar

02 **Minion-ID präparieren** – Befehl in die ID eines vermeintlichen Knotens einbetten

03 **Befehl als Root** – AutomatedProvisioner führt den eingeschleusten Befehl aus

04 **Kontrolle** – Zugriff auf Conductor, Konfiguration und gesteuerte Router

Betroffenheit & Fixversionen

Release-Zweig	Verwundbar bis	Fixversion (Ziel)
bis 7.0	< 7.0.5	7.0.5
7.1	7.1.0 – < 7.1.7	7.1.7
7.2	7.2.0 – < 7.2.3	7.2.3
Workaround	laut Juniper keiner	—

Juniper nennt im CVE-Datensatz den **Session Smart Conductor** als betroffenes Produkt; CISA führt den Eintrag unter „Session Smart Conductor and Session Smart Router“. Router-Installationen deshalb im selben Zug prüfen und den Release-Stand gegen JSA112183 abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die Netzsteuerung 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

28.10.2026
Juniper veröffentlicht JSA112183 (Oktober-Bulletin)

bis 25.11.2026
Juniper SIRT erhält Meldung über Ausnutzung

25.11.2026
Aufnahme in CISA KEV · Triage-Pflicht

28.11.2026
Ablauf der CISA-Frist (US-Behörden)

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Erreichbarkeit einschränken, patchen, dann Kompromittierung ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Zugriff einschränken	Update einspielen	Conductor auf Kompromittierung prüfen

01 Betroffenheit feststellen

Alle Session Smart Conductor (und vorsorglich die Session Smart Router) erfassen und den Release-Stand ablesen. Betroffen sind Versionen vor `7.0.5`, `7.1.0` bis vor `7.1.7` sowie `7.2.0` bis vor `7.2.3`.

02 Erreichbarkeit einschränken (vor dem Update)

Juniper nennt keinen Workaround. Bis zum Update den Conductor nur aus den Netzen erreichbar halten, aus denen sich die eigenen Router tatsächlich verbinden, und jede Freigabe ins offene Internet schließen. Das senkt das Risiko, ersetzt das Update aber nicht.

03 Patchen

Auf die bereinigte Version des eigenen Zweigs aktualisieren: `7.0.5` · `7.1.7` · `7.2.3` oder neuer. Vorher die Konfiguration sichern und die Reihenfolge Conductor vor Routern nach Juniper-Upgrade-Pfad einhalten.

04 Kompromittierung ausschließen

Ein Update schließt die Lücke, nicht einen bereits erfolgten Zugriff. Auf dem Conductor die Liste der registrierten bzw. angenommenen Knoten auf unbekannte oder ungewöhnlich benannte Minion-IDs prüfen, Systemprotokolle auf unerwartete Root-Prozesse, neue Konten, geänderte Cronjobs und ausgehende Verbindungen durchsehen und Konfigurationsänderungen mit dem Change-Log abgleichen.

05 Bei Verdacht: als kompromittiert behandeln

Beweise sichern (Logs, Konfiguration, Systemabbild), bevor neu aufgesetzt wird. Zugangsdaten, Schlüssel und Zertifikate des Conductors erneuern und die vom Conductor verteilten Konfigurationen der Router auf fremde Einträge prüfen – dokumentiert für eine etwaige Meldung.

Kompromittierungs-Indikatoren (IoCs)

KNOTEN-REGISTRIERUNG

Unbekannte oder auffällig benannte Minion-IDs (Sonderzeichen, Befehlsfragmente)

SYSTEM (CONDUCTOR)

Unerwartete Root-Prozesse, neue Konten, geänderte Cronjobs oder Dienste

NETZ

Ausgehende Verbindungen des Conductors zu unbekannten Zielen

Zur Einordnung: Juniper und CISA haben bislang keine konkreten Indikatoren (IPs, Hashes, Dateinamen) veröffentlicht. Die genannten Prüfpunkte sind allgemeine Hinweise für eine Befehlsausführung als Root und ersetzen keine forensische Analyse. Ein fehlender Treffer ist kein Ausschluss, wenn Logs rotiert oder gelöscht wurden.

Wichtig: Die Ausnutzung erfolgt ohne Anmeldung und mit Root-Rechten auf dem System, das alle angebundenen Standorte steuert. Ohne Auswertung der Systemprotokolle bleibt ein erfolgreicher Zugriff unsichtbar.

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

Worauf wir bei dieser Schwachstelle achten: Unerwartete Root-Prozesse und ausgehende Verbindungen des Conductors. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte Session Smart Conductor 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 Juniper-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 die bereinigte Version sofort anordnen und die Erreichbarkeit bis dahin einschränken.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung der Netzsteuerung 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 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-2026-103406 und dem Juniper-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Juniper Networks Security Advisory JSA112183 (CVE-Datensatz der CNA Juniper) · NVD CVE-2026-103406 · CISA Known Exploited Vulnerabilities Catalog. Angaben nach bestem Wissen zum Stand 25.11.2026; Fixversionen gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.