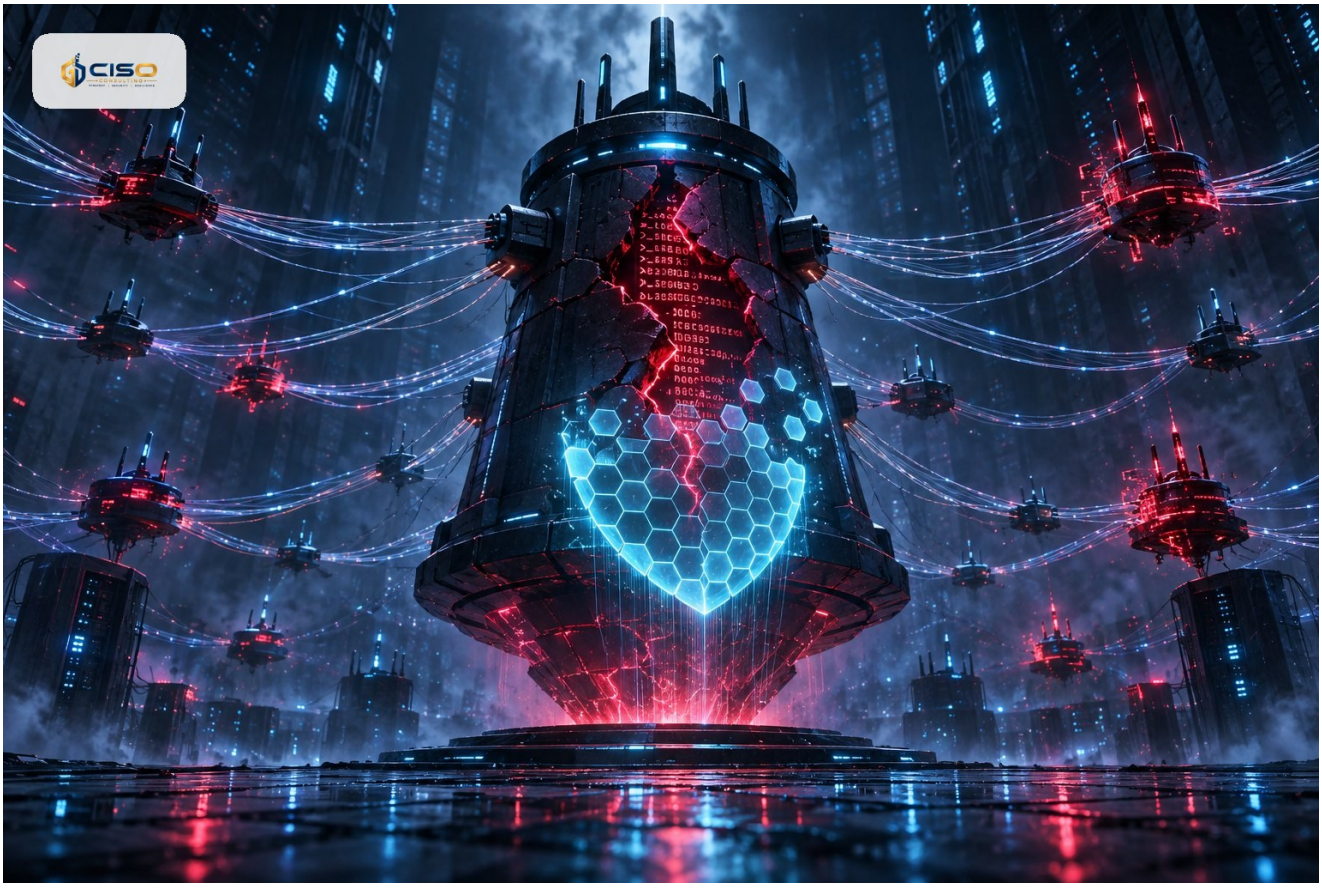
استغلال ثغرة CVE-2026-103406 في Juniper Session Smart Conductor والتصحيح متاح



أكدت Juniper وCISA استغلال الثغرة (CVSS 9.8) CVE-2026-103406 في Session Smart Conductor، وهي حقن أوامر يتيح صلاحيات الجذر. التصحيح متاح منذ 28 أكتوبر.

- الثغرة CVE-2026-103406 حقن أوامر نظام تشغيل قابل للاستغلال عن بُعد بدرجة CVSS تبلغ 9.8.
- تؤثر في خدمة AutomatedProvisioner وتتيح تنفيذ أوامر بصلاحيات الجذر عبر معرّف Salt minion مُعدّ خصيصًا.
- حدّثت Juniper نشرتها لتفيد بالإبلاغ عن حالة استغلال خبيث واحدة على الأقل لدى فريق SIRT.
- أضافت CISA الثغرة إلى كتالوج KEV، والإصدارات المصححة هي 7.2.3 و7.1.7 و7.0.5.
- صدر التصحيح في 28 أكتوبر ضمن 18 إصلاحًا في Conductorg Session Smart Router.

حذّرت Juniper Networks ووكالة CISA الأمريكية من أن مهاجمين يستغلون ثغرة حرجة في Session Smart Conductor، وهي منصة الإدارة والسياسات المركزية المستخدمة لتنسيق أجهزة Session Smart Router.

ما الذي يتأثر

الثغرة **CVE-2026-103406** (بدرجة CVSS تبلغ 9.8) هي حقن أوامر نظام تشغيل في خدمة AutomatedProvisioner. يستطيع مهاجم عن بُعد استخدام معرّف Salt minion مُعدّ خصيصًا، وهو المعرّف الذي يقدّمه الراوتر عند تسجيله لدى Salt master (أي Conductor)، لتنفيذ أوامر اختيارية بصلاحيات الجذر.

صحّحت Juniper الثغرة في 28 أكتوبر مع 17 ثغرة أخرى في Session Smart Router وSession Smart Conductor. وهذا الأسبوع حدّثت نشرتها لتصنّف الثغرة على أنها مستغلة، مشيرة إلى الإبلاغ عن حالة استغلال خبيث واحدة على الأقل لدى فريق SIRT. بعد ذلك أضافتها CISA إلى كتالوج الثغرات المستغلة المعروفة (KEV).

الإجراء المطلوب

الإصدارات المصححة هي 7.2.3 و7.1.7 و7.0.5. وتحثّ Juniper العملاء على الترقية في أسرع وقت وتطبيق إجراءات التخفيف إلى حين ذلك. أما مهلة الأيام الثلاثة من CISA فتسري على الجهات الفيدرالية المدنية الأمريكية فقط، لكن الوكالة توصي جميع المؤسسات بمراجعة قائمة KEV ومعالجة ما يخصها.

ولأن Conductor يدير الراوترات عبر الشبكة، فإن اختراقه بصلاحيات الجذر قد تكون له آثار واسعة. على المؤسسات التي تشغّل هذا المنتج التعامل مع التحديث بوصفه عاجلاً والتحقق من حالة الإصدار لديها الآن.

ما يجب فعله الآن

1. حصر جميع نسخ Session Smart Conductor وSession Smart Router والتأكد من إصداراتها.
2. الترقية إلى إصدار مصحح (7.2.3 أو 7.1.7 أو 7.0.5) بشكل عاجل وفق إجراءات التغيير الطارئ.
3. تطبيق إجراءات التخفيف المؤقتة من Juniper إذا تعذّرت الترقية الفورية.
4. مراجعة سجلات Conductor وتسجيلات الراوترات بحثًا عن معرّفات Salt minion غير متوقعة أو أوامر غير معتادة، ورفع أي اشتباه إلى فريق الاستجابة للحوادث.
5. اعتماد كتالوج KEV من CISA مصدرًا ضمن عملية إدارة الثغرات وترتيب أولويات التصحيح.