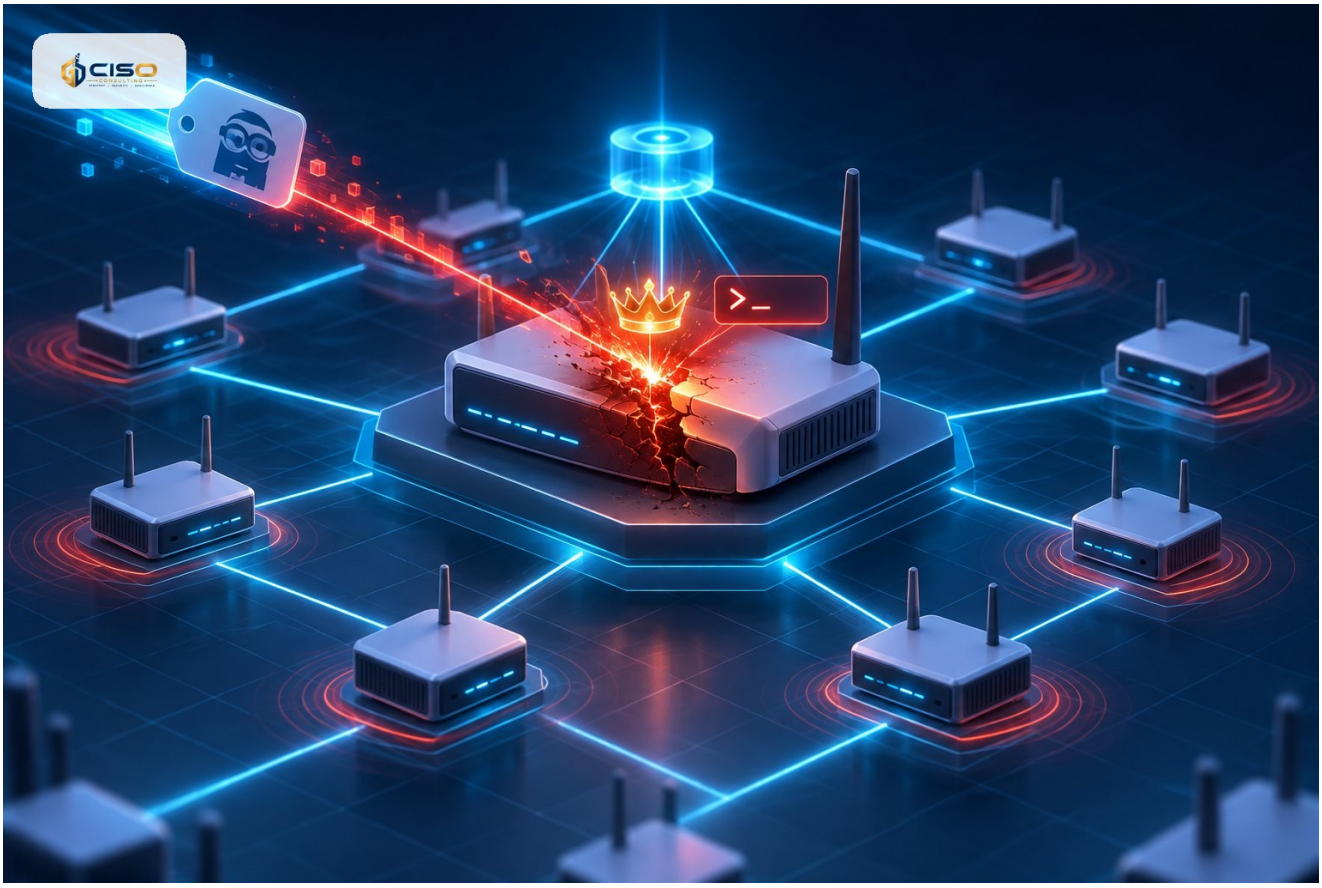
CISA تحذّر من ثغرة حقن أوامر في HPE Juniper Session Smart Routerg Session Smart Conductor



أدرجت CISA الثغرة CVE-2026-103406 في منتجي HPE Juniper Session Smart Conductor وSession Smart Routerg، وهي تتيح لمهاجم عن بُعد تنفيذ أوامر بصلاحيات root عبر معرّف salt minion مصمّم خصيصًا.

- CVE-2026-103406 ثغرة حقن أوامر في نظام التشغيل.
- تؤثر على HPE Juniper Session Smart Conductor وSession Smart Routerg.
- يمكن لمهاجم عن بُعد تنفيذ أوامر عشوائية بصلاحيات root عبر معرّف salt minion مصمّم خصيصًا.
- تشترط CISA تطبيق إجراءات التخفيف وفق تعليمات المورّد، وموعد الجهات الفيدرالية الأمريكية 28-11-2026.
- عند عدم توفر إجراءات التخفيف توجّه CISA بالتوقف عن استخدام المنتج.

أضافت CISA الثغرة CVE-2026-103406 إلى قائمة تنبيهاتها. وهي ثغرة حقن أوامر في نظام التشغيل تؤثر على HPE Juniper Session Smart Conductor وSession Smart Router.

ما الذي تتيحه الثغرة

وفق المصدر، يمكن لمهاجم عن بُعد تنفيذ أوامر عشوائية بصلاحيات root عبر تمرير معرّف salt minion مصمّم خصيصًا. وتنفيذ الأوامر بهذه الصلاحيات على موجّه أو منسّق شبكي يمنح المهاجم سيطرة كاملة على الجهاز المتأثر.

الإجراء الذي تطلبه CISA

توجّه CISA الجهات إلى تطبيق إجراءات التخفيف وفق تعليمات المورّد، والالتزام بتوجيهها BOD 26-04 بشأن تحديد أولويات التحديثات الأمنية بحسب المخاطر، إضافة إلى متطلبات الفرز الجنائي (Forensics Triage Requirements). وفي حالة الخدمات السحابية تُتبع إرشادات BOD 26-04 المعمول بها. وإذا لم تتوفر إجراءات تخفيف فيجب التوقف عن استخدام المنتج. وتقع على عاتق الجهات مسؤولية تقييم تعرّض كل أصل للإنترنت. وموعد الجهات الفيدرالية الأمريكية هو 28-11-2026.

ينطبق التوجيه والموعد رسميًا على الجهات الفيدرالية الأمريكية، لكن الخطوات مناسبة لأي مؤسسة تشغّل هذه المنتجات. ولا يذكر المصدر الإصدارات المتأثرة أو الإصدارات المصحّحة، لذا يبقى إشعار المورّد هو المرجع في هذه التفاصيل.

نظرة عملية

يُستحسن اعتبار ذلك فرصة للتحقق من وجود هذه المنتجات في بيئتكم، ومدى تعرّضها، وهل طُبّقت إجراءات المورّد، مع البدء بالأصول المتاحة من الإنترنت.

ما يجب فعله الآن

1. حصر جميع نسخ HPE Juniper Session Smart Conductor وSession Smart Router.
2. تحديد الأصول المتاحة من الإنترنت ومنحها الأولوية.
3. تطبيق إجراءات التخفيف الصادرة عن المورّد كما وردت في إشعاره.
4. إجراء فرز جنائي على النسخ المكشوفة للتحقق من أي مؤشرات اختراق.
5. عند عدم توفر إجراء تخفيف، التخطيط لإيقاف المنتج المتأثر أو عزله.
6. توثيق التقييم والمعالجة ضمن عملية إدارة الثغرات.