

CISA تنصح باتخاذ إجراءات فورية بشأن ثغرة Ivanti Connect Secure



حددت CISA ثغرة حرجية في Ivanti Connect Secure يتم استغلالها بنشاط. يُنصح المؤسسات بتحديث أنظمتها على الفور لمنع الوصول غير المصرح به وسرقة البيانات.

- تؤثر CVE-2026-104935 على إصدارات Ivanti Connect Secure 25.1.1.1 وما قبلها.
- تسمح الثغرة بتنفيذ أوامر عن بُعد دون مصادقة.
- توصي CISA بالترقية الفورية إلى الإصدار الأحدث.
- يجب على المؤسسات إجراء تحقيقات للتحقق من علامات الاختراق.
- تاريخ انتهاء الدعم للإصدار 22.8 هو 31 يناير 2027.

نظرة عامة

أصدرت CISA تنبيهًا بشأن ثغرة جديدة تم اكتشافها في Ivanti Connect Secure، المعروفة باسم CVE-2026-104935. يتم استغلال هذه الثغرة من قبل المهاجمين السيرانيين لتجاوز المصادقة، مما يمكنهم من تنفيذ أوامر عشوائية عن بُعد دون مصادقة.

الإجراءات الموصى بها

يُنصح المؤسسات التي تستخدم إصدارات متأثرة من Ivanti Connect Secure باتخاذ إجراءات فورية. تؤكد CISA على أهمية التحديث إلى الإصدار الأحدث وفقًا لإشعار الأمان من Ivanti. بالإضافة إلى ذلك، يجب على المؤسسات مراجعة دليل التوافق للحصول على تعليمات تفصيلية حول التصحيح.

بالنسبة لأولئك الذين يشعرون بالقلق بشأن احتمال الاختراق، فإن إجراء تحقيقات شاملة في الشبكة والذاكرة أمر ضروري لتحديد أي دليل على الاستغلال. لاحظ أن أداة فحص النزاهة من Ivanti قد لا تكشف عن هذه الثغرة المحددة.

خطوات التخفيف من المخاطر

إذا كان هناك اشتباه في الاختراق، يجب على المؤسسات اتباع إجراءات الاسترداد التالية:

- إنشاء نسخة احتياطية من تكوين الجهاز.
- إجراء إعادة ضبط المصنع والترقية إلى الإصدار الأحدث.
- بالنسبة للأنظمة السحابية والافتراضية، إعادة بناء النسخة الافتراضية والترقية.
- استعادة تكوين الجهاز من النسخة الاحتياطية.
- إعادة تعيين كلمات المرور لجميع الحسابات وإلغاء الشهادات المخزنة.
- إعادة تعيين مفاتيح API وبيانات اعتماد خادم الترخيص.

من خلال اتخاذ هذه الخطوات، يمكن للمؤسسات تقليل مخاطر الاستغلال بشكل كبير وتعزيز وضعها الأمني العام.

ما يجب فعله الآن

1. تحديث Ivanti Connect Secure إلى الإصدار الأحدث على الفور.
2. مراجعة إشعار الأمان من Ivanti للحصول على إرشادات تفصيلية حول التصحيح.
3. إجراء تحقيقات في الشبكة والذاكرة للتحقق من علامات الاستغلال.
4. إنشاء نسخ احتياطية من تكوينات الأجهزة.
5. إعادة تعيين كلمات المرور وإلغاء بيانات الاعتماد المخزنة.