

وكالة CISA تحت على تحديث Ivanti Connect Secure فوراً بعد رصد 105 محاولة استغلال



دعت وكالة CISA إلى تحديث أجهزة Ivanti Connect Secure فوراً بعد الاستغلال النشط لثغرة تجاوز المصادقة المسجلة برقم CVE-2026-104935.

- أصدرت وكالة CISA تنبيهاً عاجلاً بشأن أجهزة Ivanti Connect Secure بعد الكشف عن ثغرة CVE-2026-104935 لتجاوز المصادقة بدرجة خطورة 8.6 على مقياس CVSS
- سجلت أنظمة الطعم الإلكتروني 105 محاولة استغلال مما يؤكد الاستغلال النشط في البيئات الحقيقية
- تُحث المؤسسات على تحديث أنظمة ICS إلى الإصدار الأحدث فوراً
- تتيح الثغرة للمهاجمين تجاوز ضوابط المصادقة على الأجهزة المتأثرة

تأكيد الاستغلال النشط

أصدرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية تنبيهاً عاجلاً يدعو المؤسسات إلى تحديث أجهزة Ivanti Connect Secure فوراً. جاء التحذير بعد الكشف عن ثغرة **CVE-2026-104935** لتجاوز المصادقة بدرجة خطورة 8.6 على مقياس CVSS. صدر تنبيه الوكالة بعد أن سجلت أنظمة المراقبة بالطعم الإلكتروني 105 محاولة استغلال متميزة، مما يوفر دليلاً ملموساً على أن الجهات المهددة تستهدف الثغرة بنشاط في البيئات الإنتاجية.

تفاصيل الثغرة

تمثل الثغرة الأمنية نقطة ضعف في **تجاوز المصادقة** تؤثر على أنظمة Ivanti Connect Secure المنشورة. يتيح هذا النوع من الثغرات للمهاجمين تجاوز ضوابط المصادقة العادية، مما قد يمنحهم وصولاً غير مصرح به إلى الأنظمة والشبكات المحمية. تعكس درجة CVSS المرتفعة نسبياً الخطر الجسيم الذي تشكله على المؤسسات التي تشغل إصدارات ضعيفة من الجهاز.

إجراء فوري مطلوب

شددت وكالة CISA على ضرورة تطبيق التحديثات المتاحة على جميع أجهزة وأنظمة ICS. يجعل الجمع بين أدلة الاستغلال النشط وطبيعة الثغرة في تجاوز المصادقة هذا الأمر مسألة أمنية حساسة زمنياً. يجب على المؤسسات التي تستخدم Ivanti Connect Secure للوصول عن بُعد أو خدمات VPN إعطاء الأولوية للأنشطة التصحيح، خاصة بالنظر إلى دور الجهاز المعتمد كنقطة تحكم محيطية للشبكة. ينبغي للمؤسسات الخاضعة للتنظيم في المملكة التعامل مع هذا الأمر كقضية حماية بنية تحتية حرجية تتطلب اهتماماً فورياً من فرق العمليات الأمنية.

ما يجب فعله الآن

1. إجراء جرد فوري لجميع أجهزة Ivanti Connect Secure المنشورة في بيئتك
2. تطبيق أحدث التحديثات الأمنية المقدمة من المورد على جميع نسخ ICS دون تأخير
3. مراجعة سجلات المصادقة والوصول للكشف عن أي نشاط مشبوه أو محاولات وصول غير مصرح بها خلال فترة التعرض
4. تطبيق مراقبة معززة على جميع البنية التحتية للوصول عن بُعد وشبكات VPN حتى اكتمال التصحيح
5. إخطار الهيئة الوطنية للأمن السيبراني في حال اكتشاف أي مؤشرات اختراق
6. توثيق أنشطة التصحيح والجدول الزمنية لأغراض الامتثال والمراجعة