

CISA تضيف ثغرتين جديدتين إلى كتالوج الثغرات المعروفة المستغلة

CISA ADDS TWO NEW VULNERABILITIES TO KEV CATALOG



أضافت CISA ثغرتين إلى كتالوج الثغرات المعروفة المستغلة، مما يبرز الحاجة إلى أن تعطي المؤسسات الأولوية لجهود التصحيح لهذه المخاطر.

- حددت CISA ثغرتين جديدتين: ثغرة حقن الأوامر في Microsoft Windows وثغرة تجاوز المصادقة في Ivanti Connect Secure.
- تُستغل هذه الثغرات بنشاط وتشكل مخاطر كبيرة.
- يُشجع المؤسسات على اعتماد إدارة الثغرات بناءً على المخاطر.
- يعد التصحيح السريع للثغرات عالية المخاطر أمرًا ضروريًا.
- ستواصل CISA تحديث كتالوج KEV بالثغرات الجديدة.

نظرة عامة

أضافت CISA ثغرتين إلى كتالوج الثغرات المعروفة المستغلة (KEV)، مما يدل على الاستغلال النشط. تشمل الثغرات ثغرة **حقن الأوامر** في Microsoft Windows وثغرة **تجاوز المصادقة** في Ivanti Connect Secure. هذه الثغرات هي نقاط هجوم شائعة للمجرمين السيبرانيين وتشكل مخاطر كبيرة على المؤسسات.

التوصيات

بينما ينطبق التوجيه التشغيلي الملزم (BOD) 26-04 على الوكالات الفيدرالية، فإنه يسلط الضوء على أهمية إعطاء الأولوية للتصحيح للثغرات عالية المخاطر. يُشجع المؤسسات على اعتماد ممارسات مماثلة في عمليات إدارة الثغرات الخاصة بها. يتضمن ذلك تقييم المخاطر المرتبطة بكل ثغرة وإعطاء الأولوية لجهود التصحيح وفقاً لذلك.

الخطوات التالية

يجب على المؤسسات التأكد من أنها على دراية بهذه الثغرات واتخاذ الإجراءات المناسبة للتخفيف من المخاطر. يعد مراجعة كتالوج KEV بانتظام للحصول على التحديثات أمراً أساسياً للحفاظ على وضع أمني قوي.

ما يجب فعله الآن

1. مراجعة كتالوج KEV الخاص بـ CISA للحصول على أحدث الثغرات.
2. تقييم تأثير الثغرات المحددة حديثاً على أنظمتك.
3. إعطاء الأولوية لجهود التصحيح لهذه الثغرات بناءً على المخاطر.
4. تنفيذ التحديثات الأمنية بمجرد توفرها.
5. إجراء تقييمات دورية للثغرات لتحديد المخاطر المحتملة.