

CISA تضيف أربع ثغرات جديدة إلى كتالوج الثغرات المعروفة المستغلة



أضافت CISA أربع ثغرات جديدة إلى كتالوج الثغرات المعروفة المستغلة، مما يبرز الحاجة إلى أن تعطي المؤسسات الأولوية لجهود إصلاحها.

- يتضمن كتالوج KEV الخاص بـ CISA الآن أربع ثغرات جديدة تم تحديدها.
- تعتبر هذه الثغرات مستغلة بنشاط وتشكل مخاطر كبيرة.
- يتم تشجيع المؤسسات على إعطاء الأولوية لإصلاح الثغرات بناءً على المخاطر.
- تؤكد التوجيهات التشغيلية الملزمة 04-26 على الإصلاح السريع للثغرات عالية المخاطر.
- ستواصل CISA تحديث الكتالوج بإضافة ثغرات جديدة.

أضافت CISA مؤخراً أربع ثغرات إلى كتالوج الثغرات المعروفة المستغلة (KEV)، مما يشير إلى استغلالها النشط

من قبل الجهات الخبيثة. تشمل هذه الثغرات مشكلات في نظام Palo Alto Networks PAN-OS، وبوابة البريد الإلكتروني الآمن من Cisco، وAhsayCBS.

يُنصح المؤسسات بأخذ هذه الثغرات على محمل الجد، حيث تمثل نقاط هجوم شائعة يمكن أن تؤدي إلى خروقات أمنية كبيرة. تؤكد التوجيهات التشغيلية الملزمة 04-26 على أهمية إعطاء الأولوية لتحديثات الأمان بناءً على المخاطر، خاصةً بالنسبة للثغرات التي قد تسمح بالتحكم الكامل في الأنظمة المتأثرة.

بينما تنطبق التوجيهات بشكل خاص على وكالات الفرع التنفيذي المدني الفيدرالي، تشجع CISA جميع المؤسسات على اعتماد نهج قائم على المخاطر لإدارة الثغرات. يشمل ذلك معالجة الثغرات المدرجة في كتالوج KEV بسرعة، خاصة تلك التي تشكل مخاطر عالية على الأصول المعرضة للجمهور. يجب على المؤسسات أيضًا تقييم ما إذا كانت أي أنظمة قد تعرضت للاختراق قبل تطبيق التصحيحات لضمان وجود تدابير أمنية شاملة.

ما يجب فعله الآن

1. مراجعة الثغرات المضافة حديثاً في كتالوج KEV الخاص بـ CISA.
2. إعطاء الأولوية لجهود الإصلاح للثغرات عالية المخاطر.
3. تقييم تعرض مؤسستك لهذه الثغرات.
4. تنفيذ التصحيحات الأمنية بسرعة للتخفيف من المخاطر.
5. مراقبة الأنظمة بحثاً عن أي علامات على الاختراق قبل التصحيح.