

CISA تحدد ثغرات جديدة مستغلة: ضرورة اتخاذ إجراءات



أضافت CISA ثغرتين إلى سجل الثغرات المستغلة، مما يشير إلى استغلال نشط. يُنصح المؤسسات بإعطاء الأولوية لجهود الإصلاح.

- تم إضافة ثغرتين جديدتين إلى سجل KEV من CISA.
- CVE-2025-61624 يؤثر على عدة منتجات من Fortinet.
- CVE-2026-102764 يتعلق بدعم BeyondTrust عن بُعد.
- يُنصح المؤسسات بتبني إدارة الثغرات بناءً على المخاطر.
- الإصلاح السريع للثغرات عالية المخاطر أمر ضروري.

قامت CISA مؤخراً بتحديث سجل الثغرات المستغلة (KEV) بإضافة ثغرتين جديدتين يتم استغلالهما حالياً. الثغرة الأولى، CVE-2025-61624، تؤثر على عدة منتجات من Fortinet وتتعلق بمشكلة تجاوز المسار. الثانية، CVE-2026-102764، تتعلق بثغرة تجاوز المصادقة في دعم BeyondTrust عن بُعد.

تمثل هذه الثغرات مخاطر كبيرة، خاصةً لأنها تستهدف بشكل متكرر من قبل الجهات الفاعلة الخبيثة. تؤكد CISA على أهمية إعطاء الأولوية لإصلاح هذه الثغرات، خاصةً بالنسبة للمؤسسات التي تمتلك أصولاً مكشوفة علنيًا والتي قد تسمح بالتحكم الكامل بعد الاستغلال. بينما ينطبق التوجيه التشغيلي الملزم (26-04 BOD) على الوكالات الفيدرالية، تشجع CISA جميع المؤسسات على اعتماد نهج مماثل قائم على المخاطر في إدارة الثغرات. يجب على المؤسسات أن تظل يقظة واستباقية في معالجة الثغرات المدرجة في سجل KEV. ستستمر CISA في تحديث السجل بالثغرات الجديدة التي تلبى معايير الاستغلال النشط، ويُشجع على الإبلاغ عن أي ثغرات معروفة مستغلة غير مدرجة حاليًا.

ما يجب فعله الآن

1. مراجعة أنظمتك للثغرات المدرجة.
2. إعطاء الأولوية لجهود الإصلاح للثغرتين CVE-2025-61624 و CVE-2026-102764.
3. تنفيذ استراتيجية إدارة الثغرات قائمة على المخاطر.
4. متابعة تحديثات CISA للثغرات الجديدة.
5. الإبلاغ عن أي ثغرات معروفة مستغلة غير مدرجة في سجل KEV.