CISA تضيف أربع ثغرات مستغلة فعلياً في منتجات SAP وCisco وVMware وApache إلى كتالوج KEV



أضافت CISA أربع ثغرات في SAP NetWeaver وCisco Expressway وVMware vCenter وApache Roller إلى كتالوج KEV بناءً على أدلة استغلال فعلي، وتحث جميع المؤسسات على إعطائها الأولوية.

- أُضيفت أربع ثغرات إلى كتالوج KEV استناداً إلى أدلة على استغلالها فعلياً.
- المنتجات المتأثرة: SAP NetWeaver وCisco Expressway Series وVMware vCenter وApache Roller.
- أنواع الثغرات: حقن في منطق الاستعلام، وبيانات اعتماد مضمّنة في الشيفرة، وتجاوز المصادقة، وإلغاء تسلسل بيانات غير موثوقة.
- التوجيه BOD 26-04 مُلزم للجهات المدنية الاتحادية الأمريكية فقط، لكن CISA تشجع جميع المؤسسات على إدارة الثغرات وفق المخاطر.
- لا يتضمن المصدر إصدارات التحديثات ولا تفاصيل الهجمات.

أضافت CISA أربع ثغرات إلى كتالوج الثغرات المستغلة المعروفة (KEV) بعد توافر أدلة على استغلالها فعلياً.

ما الذي أُضيف

- **CVE-2025-42884**: في SAP NetWeaver، وتتعلق بعدم معالجة العناصر الخاصة بصورة سليمة في منطق استعلام البيانات.
- **CVE-2026-76466**: في Cisco Expressway Series، وتتعلق باستخدام بيانات اعتماد مضمّنة في الشيفرة.
- **CVE-2026-123890**: في VMware vCenter، وتتيح تجاوز المصادقة عبر مسار أو قناة بديلة.
- **CVE-2026-129448**: في Apache Roller، وتتعلق بإلغاء تسلسل بيانات غير موثوقة.

وتشير CISA إلى أن هذه الأنواع من الضعف تُعدّ وسيلة هجوم متكررة لدى الجهات الخبيثة.

لماذا يهم الأمر خارج القطاع الاتحادي الأمريكي

يُلزم التوجيه التشغيلي الملزم BOD 26-04 الجهات المدنية الاتحادية الأمريكية بسرعة معالجة ثغرات KEV على الأصول المكشوفة للإنترنت متى كان استغلالها يمنح سيطرة كاملة على الأصل، مع تأجيل الثغرات الأقل خطورة. كما يضع توقعات أساسية للتحقق مما إذا كان النظام قد اختُرق قبل تطبيق التصحيح.

لا ينطبق التوجيه على المؤسسات خارج تلك الجهات، لكن CISA تشجع جميع المؤسسات على اعتماد إدارة الثغرات القائمة على المخاطر وإعطاء الأولوية لثغرات الكتالوج. ويمكن لمن يعلم بثغرة مستغلة غير مدرجة تقديمها عبر نموذج الترشيح، بشرط وجود رقم CVE ودليل استغلال وإرشادات تخفيف واضحة.

نهج مقترح

لا يذكر المصدر إصدارات المعالجة ولا تفاصيل تقنية للهجمات، لذا يُرجع إلى نشرات كل مورّد للحصول على إرشادات المعالجة. ابدأوا بتحديد وجود هذه المنتجات في بيئتكم وأيّها مكشوف للإنترنت.

ما يجب فعله الآن

1. راجعوا سجل الأصول للتحقق من وجود SAP NetWeaver وCisco Expressway وVMware vCenter وApache Roller.
2. حدّدوا الأنظمة المكشوفة للإنترنت منها وتعاملوا معها كأولوية أولى.
3. اتبعوا نشرات كل مورّد لتطبيق التحديثات أو إجراءات التخفيف الخاصة بالثغرات الأربع.
4. للأنظمة المكشوفة، افحصوا السجلات وابحثوا عن مؤشرات اختراق سابقة لتطبيق التصحيح.
5. أدرجوا متابعة كتالوج KEV في عملية إدارة الثغرات لديكم لإعطاء أولوية للثغرات المدرجة.