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 لوجود أدلة على استغلالها فعلياً، وتحث جميع الجهات على إعطائها الأولوية.

- أُضيفت أربع ثغرات إلى كتالوج KEV استناداً إلى أدلة على استغلالها فعلياً: CVE-2025-42884 وCVE-2026-76466 وCVE-2026-123890 وCVE-2026-129448.
- المنتجات المتأثرة: SAP NetWeaver وCisco Expressway Series وVMware vCenter وApache Roller.
- أنواع الثغرات: معالجة غير سليمة للمدخلات الخاصة في منطق الاستعلام عن البيانات، وبيانات اعتماد مضمّنة في الشيفرة، وتجاوز المصادقة، وإلغاء تسلسل بيانات غير موثوقة.
- التوجيه التشغيلي BOD 26-04 ملزم للجهات الفيدرالية المدنية الأمريكية فقط، لكن CISA تشجع جميع الجهات على اعتماد إدارة ثغرات قائمة على المخاطر وإعطاء أولوية لثغرات KEV.

أضافت CISA أربع ثغرات إلى كتالوج الثغرات المستغلة المعروفة (KEV) بعد توفر أدلة على استغلالها في هجمات فعلية، وتشير إلى أن هذه الأنواع من الثغرات وسيلة هجوم متكررة لدى الجهات الخبيثة.

الثغرات الأربع المضافة

- CVE-2025-42884: في SAP NetWeaver، معالجة غير سليمة للمدخلات الخاصة في منطق الاستعلام عن البيانات
- CVE-2026-76466: في Cisco Expressway Series، استخدام بيانات اعتماد مضمّنة في الشيفرة
- CVE-2026-123890: في VMware vCenter، تجاوز المصادقة عبر مسار أو قناة بديلة
- CVE-2026-129448: في Apache Roller، إلغاء تسلسل بيانات غير موثوقة

لا يذكر المصدر الإصدارات المتأثرة ولا تفاصيل الإصلاح ولا ملابسات الاستغلال، لذا ينبغي الرجوع إلى نشرات الموردين للاطلاع عليها.

أهمية الأمر خارج الجهات الأمريكية

يُلزم التوجيه التشغيلي BOD 26-04 الصادر عن CISA الجهات الفيدرالية المدنية الأمريكية بسرعة معالجة ثغرات KEV على الأصول المكشوفة للإنترنت التي تمنح المهاجم سيطرة كاملة عند استغلالها، مع تأجيل الثغرات الأقل خطورة. كما يحدد توقعات أساسية للتحقق مما إذا كان النظام قد اختُرق قبل تطبيق التحديث.

لا ينطبق التوجيه على الجهات خارج تلك الفئة، غير أن CISA تشجع جميع المؤسسات على اعتماد إدارة ثغرات قائمة على المخاطر وإعطاء أولوية لثغرات الكتالوج. وللمؤسسات في المملكة، فإن الخطوة العملية هي التحقق سريعاً من استخدام أي من هذه المنتجات، ومعاملة المكشوف منها للإنترنت على أنه الأولوية الأولى.

ما يجب فعله الآن

1. راجعوا سجل الأصول للتحقق من وجود SAP NetWeaver وCisco Expressway وVMware vCenter وApache Roller.
2. أعطوا الأولوية للأنظمة المتاحة من الإنترنت، وطبّقوا إصلاحات الموردين أو إجراءات التخفيف فور توفرها.
3. راجعوا نشرات الموردين لمعرفة الإصدارات المتأثرة وإرشادات كل ثغرة.
4. في الأنظمة المكشوفة التي جرى تحديثها متأخراً، افحصوا السجلات ومؤشرات الاختراق بحثاً عن أي اختراق سابق للإصلاح.
5. أدرجوا متابعة كتالوج KEV ضمن عملية إدارة الثغرات كمحفّز للأولوية.