CISA تضيف أربع ثغرات مستغلة في Apache Roller وCisco Expressway وSAP NetWeaver وVMware vCenter إلى كتالوج KEV



أضافت CISA أربع ثغرات تمس Apache Roller وCisco Expressway وSAP NetWeaver وBroadcom VMware vCenter إلى كتالوج KEV لوجود أدلة على استغلالها فعليًا، وإحداها بدرجة CVSS تبلغ 9.8.

- أضافت CISA يوم الجمعة أربع ثغرات إلى كتالوج الثغرات المستغلة المعروفة (KEV).
- المنتجات المتأثرة: Apache Roller وCisco Expressway وSAP NetWeaver وBroadcom VMware vCenter.
- استندت CISA إلى أدلة على استغلال نشط للثغرات الأربع.
- إحدى الثغرات، CVE-2026-129448، بدرجة CVSS 9.8 وتتعلق بإلغاء تسلسل بيانات غير موثوقة.

- يشير عنوان المصدر إلى هجمات تجسس ناشئة، لكن المقتطف المتاح لا يقدم تفاصيل إضافية.

أضافت الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية (CISA) أربع ثغرات إلى كتالوج الثغرات المستغلة المعروفة (KEV)، مشيرة إلى وجود أدلة على استغلالها فعليًا.

ما الذي أُضيف

المنتجات المتأثرة هي Apache Roller وCisco Expressway وSAP NetWeaver وBroadcom VMware vCenter. ولا يفصّل المقتطف المتاح سوى ثغرة واحدة هي CVE-2026-129448 بدرجة CVSS تبلغ 9.8، وتتعلق بإلغاء تسلسل بيانات غير موثوقة. أما بقية المعرّفات والأوصاف التقنية فلم ترد في المادة المتاحة لنا، لذلك لا نوردها هنا.

كما يشير عنوان المصدر إلى هجمات تجسس ناشئة بالتزامن مع هذا الاستغلال. ولا يذكر المقتطف الجهة المسؤولة ولا القطاعات المستهدفة ولا كيفية الربط بين الثغرات، ولذلك لا ينبغي افتراض أي إسناد.

لماذا يهمّ ذلك

إدراج ثغرة في KEV يعني أن الاستغلال يجري الآن وليس نظريًا فقط. وغالبًا ما تحتل منتجات مثل إدارة الافتراضية وبوابات الاتصال ومنصات التطبيقات المؤسسية مواقع ذات صلاحيات واسعة، لذا ينبغي للمؤسسات التي تشغّل أيًّا منها التحقق سريعًا من تعرضها.

نهج مقترح

تأكدوا من وجود المنتجات المتأثرة في بيئتكم، بما فيها ما يديره أطراف ثالثة، ثم راجعوا نشرة كل مورّد لمعرفة الإصدارات المصححة والإجراءات المخففة. وأعطوا الأولوية للأنظمة المكشوفة للإنترنت وطبقات الإدارة، وراجعوا السجلات بحثًا عن نشاط غير معتاد إلى حين تطبيق التحديثات.

ما يجب فعله الآن

1. راجعوا سجل الأصول للتحقق من وجود Apache Roller وCisco Expressway وSAP NetWeaver وVMware vCenter، بما في ذلك الأنظمة التي يديرها أطراف ثالثة.
2. اطلعوا على نشرة الأمان لدى كل مورّد وطبّقوا الإصدارات المصححة أو الإجراءات المخففة، بدءًا بالأنظمة المكشوفة للإنترنت وأنظمة الإدارة.
3. أدرجوا الثغرات الأربع في متابعة إدارة الثغرات مع مهلة معالجة قصيرة.
4. افحصوا السجلات والتنبيهات على الأنظمة المتأثرة بحثًا عن مؤشرات اختراق قبل التحديث وبعده.
5. قيّدوا الوصول إلى واجهات الإدارة بالشبكات الموثوقة إذا تعذّر التحديث الفوري.