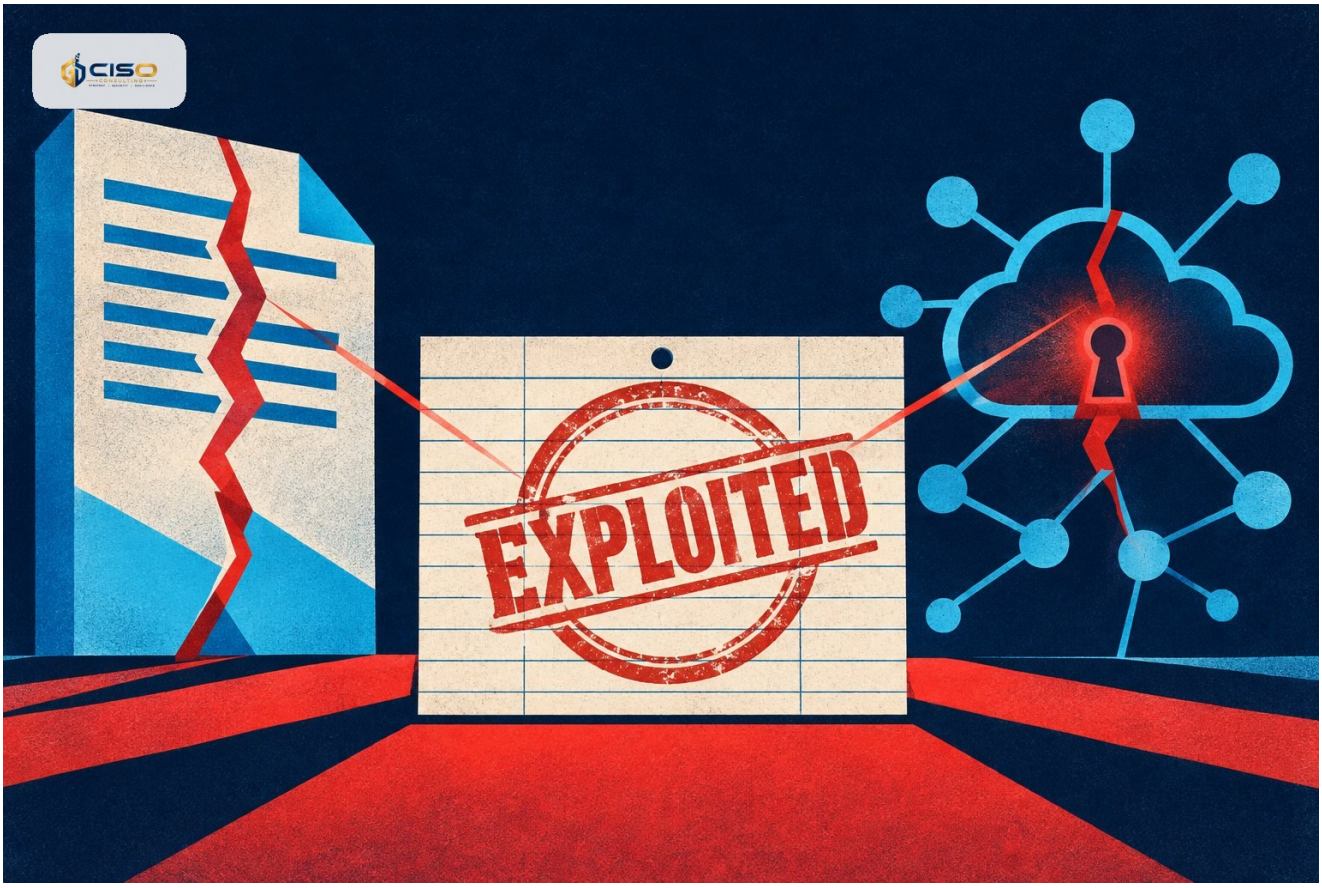
CISA تضيف ثغرتين حرجتين في Collabora Online وArista VeloCloud إلى قائمة الثغرات المستغَلة



أضافت CISA ثغرتين حرجتين في Collabora Online Built-in CODE Server وArista VeloCloud Orchestrator إلى كتالوج KEV بعد ورود تقارير عن استغلالهما فعليًا، إحداهما CVE-2026-110447 بدرجة CVSS 9.2.

- أضافت CISA ثغرتين إلى كتالوج الثغرات المعروفة والمستغَلة (KEV).
- المنتجان المتأثران هما Collabora Online Built-in CODE Server وArista VeloCloud Orchestrator (VCO).
- تستند CISA إلى تقارير عن استغلال فعلي للثغرتين.
- تصنَّف الثغرتان حرجتين، وتبلغ درجة CVE-2026-110447 وفق CVSS 9.2.
- المقتطف المتاح من المصدر لا يتضمن تفاصيل تقنية كاملة أو معلومات عن التحديثات.

ما الذي أُعلن

أضافت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) يوم الجمعة ثغرتين إلى كتالوج الثغرات المعروفة والمستغَلة (KEV)، مستندةً إلى تقارير تفيد باستغلالهما فعليًا.

المنتجان المتأثران هما Collabora Online Built-in CODE Server وVCO (Arista VeloCloud Orchestrator).
وتصنَّف الثغرتان حرجتين، وإحداهما CVE-2026-110447 بدرجة CVSS تبلغ 9.2.

ما لا يزال غير معروف

المقتطف المتاح من المصدر محدود؛ فهو لا يذكر رقم الثغرة الثانية ولا الإصدارات المتأثرة ولا أسلوب الهجوم ولا حالة الإصلاحات من الجهتين المصنِّعتين. لذلك ينبغي الرجوع إلى نشرات الموردين وإدخالات KEV لدى CISA للحصول على هذه التفاصيل بدل افتراضها.

أهمية الأمر

إدراج ثغرة في KEV يعني أن استغلالها وقع فعلاً وليس نظريًا. وبالنسبة للجهات التي تستخدم هذين المنتجين في التعاون على المستندات أو إدارة شبكات الاتصال الواسعة، فالخطوة المناسبة هي التحقق سريعًا من التعرض ثم ترتيب المعالجة وفق توجيهات المورد.

الخطوات المقترحة

- التحقق من وجود أي من المنتجين، بما في ذلك بيئات الاختبار والفروع.
- مراجعة نشرات الموردين وتطبيق الإصلاحات أو الإجراءات التخفيفية.
- البحث عن مؤشرات اختراق حيثما كان المنتج متاحًا من شبكات غير موثوقة.

ما يجب فعله الآن

1. حصر جميع نُسخ Collabora Online CODE Server وArista VeloCloud Orchestrator، بما فيها بيئات الاختبار والفروع.
2. مراجعة نشرات الموردين وإدخالات KEV لدى CISA لتأكيد الإصدارات المتأثرة والإصلاحات المتاحة.
3. تطبيق التحديثات أو الإجراءات التخفيفية بصفة طارئة على أي نسخة معرّضة.
4. تقييد الوصول من الإنترنت إلى واجهات الإدارة والتعاون قدر الإمكان.
5. مراجعة سجلات هذه الأنظمة بحثًا عن نشاط غير معتاد، والتصعيد عبر مسار الاستجابة للحوادث عند رصده.