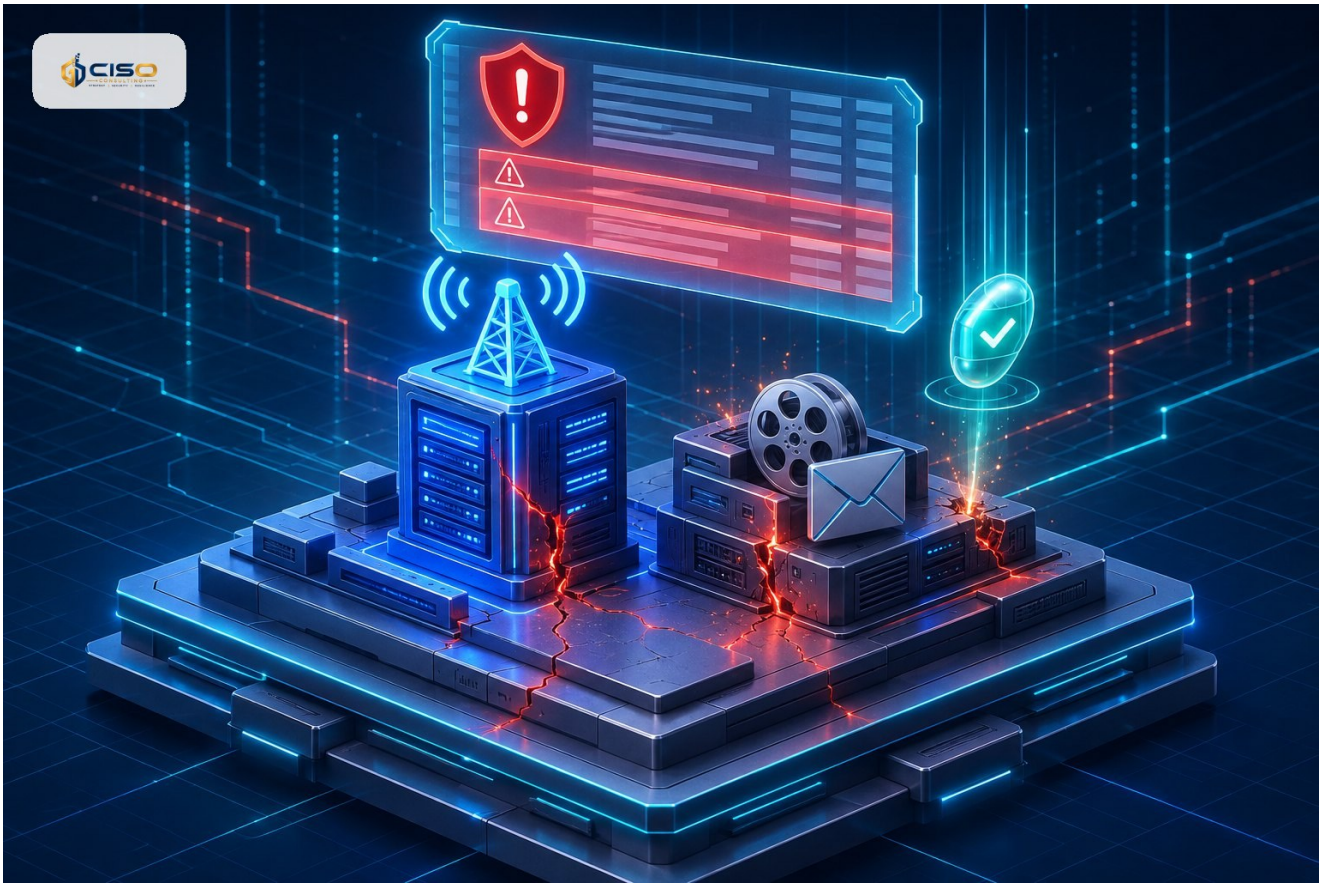
CISA تضيف ثغرتين في Cisco BroadWorks وOpenwave إلى قائمة الثغرات المستغلة



أضافت CISA ثغرتين في Cisco BroadWorks Openwave Messaging Webtop Mediag Transcoder إلى كتالوج الثغرات المستغلة، مع وجود أدلة على استغلالها فعلياً. التحديثات متاحة ويُنصح بتطبيقها.

- أضافت CISA ثغرتين إلى كتالوج KEV استناداً إلى أدلة على استغلالهما الفعلي.
- المنتجان المتأثران هما Cisco BroadWorks Openwave Messaging Webtop Mediag Transcoder.
- إحدى الثغرتين CVE-2026-20320 بدرجة CVSS تبلغ 7.5 وتتعلق بتقييد غير سليم للمراجع الخارجية في XML.
- العنوان يشير إلى أن التحديثات متاحة رغم استمرار الاستغلال.

ما الذي حدث

أضافت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) ثغرتين أمنيتين إلى كتالوج الثغرات المستغلة المعروفة (KEV)، مشيرة إلى وجود أدلة على استغلالهما فعلياً. والمنتجان المتأثران هما Cisco BroadWorks وOpenwave Messaging Webtop Media Transcoder.

إحدى الثغرتين هي **CVE-2026-20320** بدرجة CVSS تبلغ 7.5، وتُوصف بأنها تقييد غير سليم للمراجع الخارجية للكيانات في XML. أما المقتطف المتاح من المصدر فلا يتضمن تفاصيل الثغرة الثانية ولا طبيعة الاستغلال ولا الجهات المستهدفة، لذلك لا نخمّن بشأنها.

لماذا يهم ذلك

إدراج ثغرة في كتالوج KEV يعني أن استغلالها وقع فعلًا. ويذكر المصدر أن التحديثات متاحة، ما يعني أن مستوى التعرض يعتمد إلى حد كبير على سرعة تطبيقها. وغالباً ما تكون منصات الاتصالات من هذا النوع متاحة عبر الإنترنت، لذا تستحق النسخ غير المحدّثة اهتماماً مبكراً.

الخطوات المقترحة

تحقق من وجود أي من المنتجين في بيئتكم، بما في ذلك النسخ التي يديرها مزودو الخدمة نيابة عنكم. وإن وُجدا، فراجعوا نشرات الشركات المصنّعة لمعرفة الإصدارات المصححة، وجدولوا التحديث بأولوية. وإذا تعذّر التحديث فوراً، فراجعوا نطاق التعرض وراقبوا أي نشاط غير معتاد.

ما يجب فعله الآن

1. تحققوا من سجل الأصول وترتيبات مزودي الخدمة بشأن وجود Cisco BroadWorks وOpenwave Messaging Webtop Media Transcoder.
2. راجعوا نشرات الشركات المصنّعة للثغرة CVE-2026-20320 والثغرة الثانية وحدّدوا الإصدارات المصححة.
3. أعطوا أولوية لتحديث النسخ المتأثرة، بدءاً بالمتاحة عبر الإنترنت.
4. عند تأخر التحديث، قيّدوا الوصول إلى الأنظمة وكثّفوا مراقبتها.
5. أدرجوا مدخلات CISA KEV ضمن عملية إدارة الثغرات لتصعيد الثغرات المستغلة.