CISA تضيف ثغرة Cisco BroadWorks المستغلة CVE-2026-20320 إلى كتالوج KEV



أكدت CISA استغلال الثغرة CVE-2026-20320 في Cisco BroadWorks، وهي ثغرة XXE دون مصادقة تكشف بيانات الإعدادات. أصدرت Cisco التصحيح في أغسطس، وعلى مشغلي المنصة التحقق من تطبيقه.

- CVE-2026-20320 ضعف من نوع XXE في محلل XML الخاص بواجهة OCI في Cisco BroadWorks، ويمكن استغلاله عن بعد دون مصادقة.
- أضافته CISA إلى كتالوج KEV وحددت 24 نوفمبر موعدًا نهائيًا للجهات الفيدرالية الأمريكية.
- أصدرت Cisco التصحيح في أغسطس، وتعود الثغرة إلى تفعيل حل الكيانات الخارجية افتراضيًا.
- أفادت Malbear Labs بهجوم على مزود اتصالات أوروبي وثلاث عشرة جهة تستخدم بنيته، جرى فيه الحصول على مفاتيح وشهادات.
- تحث CISA فرق الأمن في القطاع الخاص أيضًا على إعطاء أولوية لثغرات KEV.

حذّرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) من أن الثغرة **CVE-2026-20320** عالية الخطورة في Cisco BroadWorks تُستغل في هجمات فعلية. وBroadWorks منصة اتصالات موحدة سحابية يستخدمها مشغلو الاتصالات ومزودو الخدمات المُدارة لتقديم خدمات المقسم السحابي والصوت والتعاون لعملائهم من الشركات.

ما هو معروف

تتمثل الثغرة في ضعف XXE (الكيانات الخارجية في XML) داخل محلل XML الخاص بواجهة Open Client Interface (OCI)). يستطيع مهاجم عن بعد ودون مصادقة إرسال رسالة XML مصممة خصيصًا إلى خدمة OCI-P وقراءة معلومات إعدادات حساسة. وأوضحت Cisco أن حل الكيانات الخارجية كان مسموحًا افتراضيًا، وقد أصدرت التصحيح في أغسطس.

أضافت CISA الثغرة إلى كتالوج الثغرات المستغلة المعروفة (KEV) وألزمت الجهات المدنية الفيدرالية الأمريكية بالمعالجة قبل 24 نوفمبر. ويقتصر هذا الإلزام على تلك الجهات، لكن CISA شجعت جميع المنظمات على اعتماد إدارة ثغرات قائمة على المخاطر وإعطاء الأولوية لثغرات KEV.

وذكرت شركة استخبارات التهديدات Malbear Labs أن جهة تهديد ناطقة بالصينية استغلت الثغرة بمساعدة نموذج ذكاء اصطناعي جرى كسر قيوده، ضد مزود اتصالات أوروبي وثلاث عشرة جهة تستخدم مراكز بياناته وبنيته السحابية. ووفق الشركة، حصل المهاجم من مضيف XSP على المفتاح الخاص لهوية النظام وعدة مجموعات بيانات اعتماد SSL ومفاتيح خاصة إضافية. ويُستخدم مفتاح هوية النظام للمصادقة بين مكونات المنصة، ما يتيح انتحال هوية XSP. كما وجدت أن خادم Provisioning كان مكشوفًا عبر قائمة أدلة دون مصادقة.

ما العمل

على المنظمات التي تشغّل BroadWorks أو تعتمد على مزود يشغّله التأكد من تطبيق تصحيح أغسطس ومراجعة احتمال تعرض بيانات اعتماد للكشف.

ما يجب فعله الآن

1. تأكد مع فريق تقنية المعلومات أو مزود الاتصالات/الخدمات المُدارة من استخدام BroadWorks ومن تطبيق تصحيح Cisco الصادر في أغسطس.
2. قيّد الوصول الشبكي إلى خدمة OCI-P (المنفذ 2208 بحسب Malbear Labs) بحيث يقتصر على شبكات الإدارة الموثوقة.
3. عند الاشتباه بالتعرض، بدّل مفتاح هوية النظام وبيانات اعتماد SSL والمفاتيح الخاصة وأعد إصدار الشهادات.
4. تحقق من أن أدلة خادم Provisioning غير قابلة للعرض العام.
5. أدرج ثغرات كتالوج KEV ضمن أولويات إدارة الثغرات واطلب من الأطراف الثالثة تأكيد تطبيق التصحيحات.