CISA تضيف ثغرتين مستغلتين في GitLab وCisco إلى كتالوج KEV



أضافت CISA ثغرتين مستغلتين فعليًا في منتجات Cisco وGitLab إلى كتالوج KEV، إحداهما CVE-2026-97229 في GitLab بدرجة CVSS تبلغ 10.0. والمقتطف المتاح لا يتضمن تفاصيل أخرى كثيرة.

- أضافت CISA ثغرتين تخصان Cisco وGitLab إلى كتالوج الثغرات المستغلة المعروفة (KEV).
- استندت الإضافة إلى أدلة على استغلال فعلي.
- الثغرة CVE-2026-97229 هي تجاوز عددي صحيح (integer overflow or wraparound) في GitLab Community Edition وEnterprise بدرجة CVSS تبلغ 10.0.
- يصف العنوان ثغرة GitLab بأنها تنفيذ شيفرة عن بُعد، وثغرة Cisco بأنها حجب خدمة في جدار الحماية.
- لا يذكر المقتطف رقم الثغرة الثانية ولا تفاصيل التصحيحات.

أضافت الوكالة الأمريكية للأمن السيبراني وأمن البنية التحتية (CISA) ثغرتين تمسّان منتجات Cisco وGitLab إلى كتالوج الثغرات المستغلة المعروفة (KEV)، مشيرةً إلى وجود أدلة على استغلالهما فعليًا.

ما المعروف حتى الآن

الثغرة الأولى هي **CVE-2026-97229**، وهي ثغرة تجاوز عددي صحيح (integer overflow or wraparound) في GitLab Community Edition وEnterprise، بدرجة CVSS تبلغ 10.0. ووفق عنوان المصدر، تتيح ثغرة GitLab تنفيذ شيفرة عن بُعد، بينما تتعلق ثغرة Cisco بحجب الخدمة في جدران الحماية.

لا يتضمن المقتطف المتاح لنا معرّف الثغرة الخاصة بـ Cisco ولا الإصدارات المتأثرة ولا الإصدارات المصححة، لذلك لا نخوض في هذه التفاصيل، ونوصي بالرجوع مباشرة إلى نشرات الشركتين.

لماذا يهم ذلك

إدراج ثغرة في KEV يعني أن الاستغلال رُصد فعلاً، فتنتقل من خطر نظري إلى أولوية تشغيلية. وتستحق ثغرة بدرجة قصوى في منصة إدارة الشيفرة المصدرية اهتمامًا خاصًا، إذ تحتفظ هذه المنصات عادةً بالشيفرة وبيانات الاعتماد وصلاحيات خطوط النشر. أما حجب الخدمة في جدار حماية طرفي فقد يؤثر على توافر الخدمات المحمية.

على الجهات التي تشغّل أيًّا من المنتجين التحقق من تعرضها واتباع إرشادات الشركتين دون انتظار مزيد من التقارير.

ما يجب فعله الآن

1. حصر جميع نسخ GitLab Community Edition وEnterprise وجدران حماية Cisco في بيئتكم، وخاصة المكشوفة على الإنترنت.
2. مراجعة نشرات GitLab وCisco بشأن CVE-2026-97229 وثغرة Cisco، وتطبيق التصحيحات أو المعالجات المؤقتة وفق التوجيهات.
3. إعطاء الأولوية لنسخ GitLab نظرًا لدرجة CVSS البالغة 10.0 وتأكد الاستغلال.
4. فحص سجلات GitLab وجدران الحماية بحثًا عن نشاط غير معتاد، وتدوير الأسرار المخزنة في النسخ المتأثرة عند الاشتباه باختراق.
5. إدراج متابعة كتالوج KEV ضمن عملية إدارة الثغرات وتوثيق قرارات التصحيح لأغراض التدقيق.