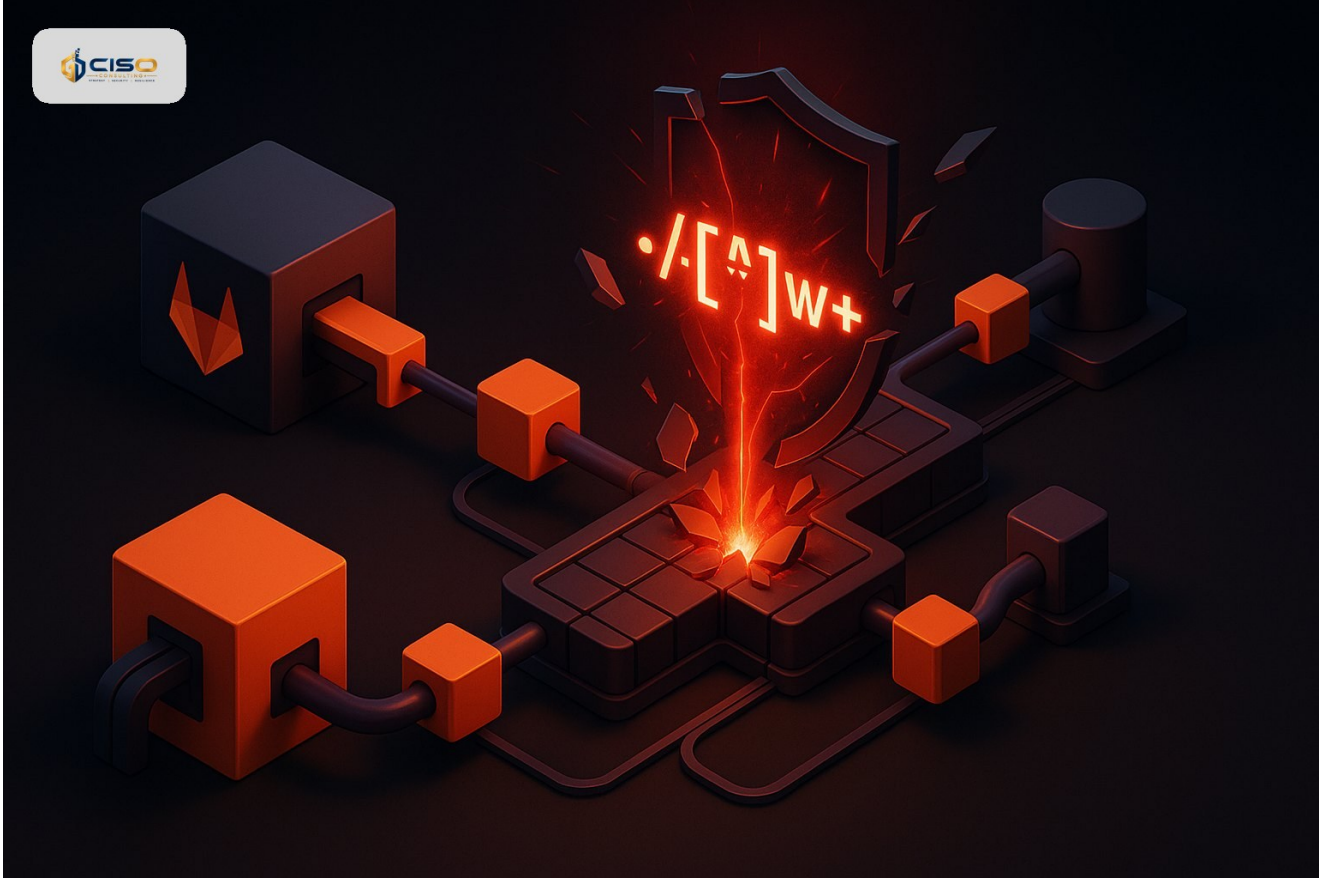


GitLab تصدر تحديثات أمنية لمعالجة ثغرة بالغة الخطورة تتيح تنفيذ أوامر عن بُعد في مُجمّع التعبيرات النمطية



أصدرت GitLab تحديثات أمنية لمعالجة ثغرة حرجية تتيح تنفيذ أوامر برمجية عن بُعد دون مصادقة عبر تعبيرات نمطية ضارة في ملفات تهيئة CI/CD.

- الثغرة CVE-2026-97229 هي عيب فائض عدد صحيح بالغ الخطورة في مُجمّع التعبيرات النمطية لـ CI/CD في GitLab يتيح تنفيذ أوامر عن بُعد
- يمكن للمهاجمين غير المصادق عليهم استغلال الثغرة باستخدام تعبيرات نمطية مصممة خصيصاً في ملفات تهيئة خطوط الأنابيب
- صدرت تحديثات أمنية لإصدارات GitLab CE و EE بأرقام 19.2.8 و 19.3.4 و 19.4.2؛ وتم تحديث GitLab.com بالفعل
- تم الإبلاغ عن الثغرة عبر برنامج مكافآت الثغرات HackerOne من قبل الباحث 'joaxcar'
- عالجت GitLab عدة ثغرات بالغة الخطورة في الأشهر الأخيرة، وأدرجت CISA خمس ثغرات

تفاصيل الثغرة الأمنية

أصدرت GitLab تحديثات أمنية عاجلة لمعالجة الثغرة **CVE-2026-97229** باللغة الخطورة في مُجمّع التعبيرات النمطية الخاص بـ CI/CD. تنشأ الثغرة من ضعف فائض عدد صحيح يتيح للمهاجمين عن بُعد دون مصادقة تنفيذ أوامر برمجية تعسفية على نُسخ GitLab المعرضة للخطر. تؤثر الثغرة على المكوّن المسؤول عن تحليل وتجميع وتقييم التعبيرات النمطية في ملفات تهيئة خطوط الأنايب للمشاريع.

وفقاً للنشرة الأمنية من GitLab، يمكن للثغرة أن تتيح للمهاجمين تشغيل أوامر على خوادم GitLab عبر تعبيرات نمطية مصممة خصيصاً في تهيئات CI/CD بسبب عدم كفاية التحقق من الصحة. اكتشف الثغرة باحث أمني يستخدم اسم 'joaxcar' وأبلغ عنها عبر برنامج مكافآت الثغرات HackerOne التابع لـ GitLab.

الإصدارات المتأثرة والمعالجة

تؤثر الثغرة الأمنية على إصدارات GitLab Community Edition و Enterprise Edition من 19.2 قبل 19.2.8، ومن 19.3 قبل 19.3.4، ومن 19.4 قبل 19.4.2. أصدرت GitLab تحديثات لجميع الإصدارات المتأثرة وتوصي بشدة بالترقية الفورية لجميع التثبيتات ذاتية الإدارة. أكدت الشركة أن GitLab.com يعمل بالفعل بالإصدار المُحدّث، بينما لا يحتاج عملاء GitLab Dedicated إلى اتخاذ إجراء.

السياق الأوسع

تُعد هذه الثغرة الأحدث في سلسلة من المشكلات الأمنية الحرجة التي تؤثر على GitLab. في يناير، عالجت المنصة ثغرة تجاوز المصادقة الثنائية عالية الخطورة (CVE-2026-0723)، وفي الشهر الماضي عالجت ثغرة أخرى باللغة الخطورة (CVE-2026-85706) تتيح سرقة البيانات دون مصادقة. أضافت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية CISA الثغرة CVE-2026-85706 إلى كتالوج الثغرات المُستغلة بعد يوم واحد من الإفصاح، وأمرت الوكالات الفيدرالية بالتحديث خلال ثلاثة أيام. أدرجت CISA خمس ثغرات في GitLab مُستغلة في هجمات منذ نوفمبر 2021، بما في ذلك واحدة استخدمتها مجموعات برمجيات الفدية.

تفيد GitLab بأن لديها أكثر من 30 مليون مستخدم مسجل واعتماد من أكثر من نصف شركات Fortune 100.

ما يجب فعله الآن

1. تحديد جميع نُسخ GitLab Community Edition و Enterprise Edition ذاتية الإدارة ضمن البنية التحتية لمؤسستك
2. الترقية الفورية لُسخ GitLab المتأثرة إلى الإصدارات المُحدّثة 19.2.8 أو 19.3.4 أو 19.4.2 حسب فرع الإصدار الحالي
3. مراجعة سجلات الوصول إلى GitLab للبحث عن تهيئات مشبوهة لخطوط أنابيب CI/CD أو أنماط تعبيرات نمطية غير عادية مُقدّمة قبل التحديث
4. التحقق من أن نُسخ GitLab غير معرّضة مباشرة للإنترنت دون ضوابط أمنية إضافية مثل VPN أو قوائم عناوين IP المسموحة

5. توثيق نشاط التحديث والجدول الزمني لسجلات الامتثال بموجب متطلبات الضوابط الأساسية للأمن السيرياني أو إطار الأمن السيرياني لمؤسسة النقد
6. إحاطة فرق التطوير وDevOps بالثغرة لضمان الوعي بممارسات تهيئة CI/CD الآمنة