ثغرة حرجة في GitLab CE/EE (CVE-2026-97229) تتيح تنفيذ تعليمات برمجية دون مصادقة



أصدرت GitLab في 12 أكتوبر 2026 إصلاحات لـ 24 مشكلة أمنية، منها ثغرة بدرجة CVSS 10.0 تتيح لمهاجم غير موثّق تنفيذ تعليمات برمجية على الخادم. ويوصي CERT-EU بالترقية، بدءًا بالنسخ المكشوفة للإنترنت.

- الثغرة CVE-2026-97229 (CVSS 10.0) في مترجم التعابير النمطية ضمن CI/CD وتتيح تنفيذ تعليمات برمجية عن بُعد دون مصادقة.
- المتأثر: نسخ GitLab CE/EE المستضافة ذاتيًا قبل 19.4.2 و19.3.4 و19.2.8.
- الإصدارات المصححة هي 19.4.2 و19.3.4 و19.2.8 وقد صدرت في 12 أكتوبر 2026.
- يعالج الإصدار أيضًا ثغرة XSS (CVSS 8.7) وثغرة صلاحيات على الفروع المحمية (CVSS 8.5) وخللاً في تسميم الذاكرة المؤقتة (8.2) قد يكشف متغيرات CI/CD المحمية.
- يوصي CERT-EU بترقية النسخ المكشوفة للإنترنت أولاً.

أصدرت GitLab الإصدارات 19.4.2 و19.3.4 و19.2.8 من النسختين Community وEnterprise، وتعالج هذه التحديثات 24 مشكلة أمنية، إحداها حرجة. وقد نشر CERT-EU نشرة بشأن هذا الإصدار في 12 أكتوبر 2026.

الثغرة الحرجة

تبلغ درجة **CVE-2026-97229** وفق CVSS 10.0، وتقع في مترجم التعابير النمطية ضمن CI/CD. فضعف التحقق من هذه التعابير يؤدي إلى تجاوز عدد صحيح، ثم يمكن لتعبير مُعدّ خصيصًا داخل إعدادات CI/CD أن يتسبب في تنفيذ تعليمات برمجية. وبذلك يستطيع مهاجم غير موثّق تنفيذ تعليمات برمجية عشوائية على الخادم.

إصلاحات أخرى في الإصدار نفسه

- CVE-2026-92883) CVSS 8.7): ثغرة XSS في إبراز الصياغة تتيح لمستخدم موثّق تشغيل JavaScript في متصفحات مستخدمين آخرين عبر مستودع مُعدّ لهذا الغرض.
- CVE-2026-16301) CVSS 8.5): خلل في التفويض يسمح لمطوّر بتشغيل خطوط المعالجة على فروع محمية دون إذن.
- 21 مشكلة إضافية، منها خلل تسميم الذاكرة المؤقتة بدرجة 8.2 قد يكشف متغيرات CI/CD المحمية.

الإجراء المطلوب

تؤثر الثغرات في نسخ GitLab CE/EE المستضافة ذاتيًا قبل 19.4.2 أو 19.3.4 أو 19.2.8. ويوصي CERT-EU بشدة بترقية جميع هذه النسخ إلى إصدار مصحح في أقرب وقت، بدءًا بالمكشوفة للإنترنت. وعلى المؤسسات تحديد مواقع استضافة GitLab والتأكد من الإصدار العامل وجدولة الترقية دون تأخير.

ما يجب فعله الآن

1. حصر جميع نسخ GitLab CE/EE المستضافة ذاتيًا وتوثيق إصداراتها.
2. الترقية إلى 19.4.2 أو 19.3.4 أو 19.2.8 بحسب خط الإصدار المستخدم، بدءًا بالنسخ المكشوفة للإنترنت.
3. إن تعذّر التحديث فورًا، تقييد الوصول الشبكي إلى النسخة بنطاقات موثوقة.
4. بعد التحديث، مراجعة إعدادات CI/CD وسجل تشغيل خطوط المعالجة بحثًا عن تغييرات أو أنشطة غير متوقعة.
5. النظر في تدوير متغيرات CI/CD المحمية عند الاشتباه بكشفها بسبب خلل الذاكرة المؤقتة.
6. توثيق التغيير ضمن عملية إدارة الثغرات والتحديثات.