CERT-EU: ثغرة حرجة في GitLab برقم CVE-2026-110264 تتيح تنفيذ الأوامر دون مصادقة



أفاد CERT-EU بوجود ثغرة حرجة في GitLab برقم CVE-2026-110264 (درجة CVSS تبلغ 10) تتيح لمستخدم غير موثّق تنفيذ تعليمات برمجية على الخادم. تتوفر إصدارات مصححة، وتُعطى الأولوية للنسخ المكشوفة للإنترنت.

- نشرت GitLab نشرتها الأمنية في 21 أكتوبر 2026، وأصدر CERT-EU تنبيهه في 22 أكتوبر 2026.
- الثغرة CVE-2026-110264 هي تجاوز عددي صحيح في مترجم التعابير النمطية، بدرجة CVSS تبلغ 10.
- قد تتيح للمهاجم غير الموثّق تنفيذ تعليمات برمجية دون قيود على خادم GitLab المتأثر.
- تشمل الإصدارات المتأثرة Community وEnterprise عبر عدة فروع، وتُعالَج في 18.11.13 و19.0.10 و19.1.9 و19.2.9 و19.3.6 و19.4.3 و19.5.1.
- عالجت GitLab أيضاً 2 ثغرتين عاليتي الخطورة و5 متوسطة و4 منخفضة، ونشرت قاعدتي كشف.

نشر CERT-EU التنبيه 2026-019 بشأن ثغرة حرجة في إصدارَي GitLab Community وEnterprise، وذلك عقب إصدار أمني من GitLab في 21 أكتوبر 2026 عالج عدة ثغرات.

ما الذي يتأثر

الثغرة **CVE-2026-110264** هي تجاوز عددي صحيح في مترجم التعابير النمطية، وتبلغ درجتها 10 وفق CVSS. ويمكن لمستخدم غير موثّق استغلالها لتنفيذ تعليمات برمجية على خادم GitLab المتأثر.

الإصدارات المتأثرة هي من 7.0 حتى ما قبل 18.11.13، وفروع x.19 التي تسبق الإصدارات المصححة التالية:

- 19.0 قبل 19.0.10
- 19.1 قبل 19.1.9
- 19.2 قبل 19.2.9
- 19.3 قبل 19.3.6
- 19.4 قبل 19.4.3
- 19.5 قبل 19.5.1

كما عالج الإصدار نفسه ثغرتين عاليتي الخطورة و5 متوسطة و4 منخفضة.

توصيات CERT-EU

يوصي CERT-EU بتحديث الأصول المتأثرة بأسرع وقت، مع البدء بالأصول المكشوفة للإنترنت، وإجراء تقييم للكشف عن أي أصول قد تكون تعرضت للاختراق. وقد نشرت GitLab قاعدتي كشف لمحاولات الاستغلال يمكن الاستعانة بهما في هذا التقييم.

ولأن خوادم GitLab تحتوي عادةً على الشيفرة المصدرية وخطوط النشر وبيانات الاعتماد، ينبغي التعامل مع الأمر كمهمة عاجلة للترقيع والمراجعة، وتوثيق نتائجها لأغراض الحوكمة.

ما يجب فعله الآن

1. حصر جميع نسخ GitLab Community وEnterprise ومقارنة إصداراتها بالإصدارات المصححة.
2. ترقية النسخ المعرضة للثغرة إلى إصدار مصحح، بدءاً بالخوادم المكشوفة للإنترنت.
3. تفعيل قاعدتي الكشف الصادرتين عن GitLab في أدوات المراقبة ومراجعة السجلات السابقة بحثاً عن محاولات استغلال.
4. إجراء تقييم للاختراق على النسخ المكشوفة، وتغيير الأسرار والرموز المخزنة في GitLab عند الاشتباه بوقوع اختراق.
5. توثيق نتائج الترقيع والتقييم ضمن عمليات إدارة الثغرات وإدارة التغيير.