محاولة استغلال ثغرة GitLab بدرجة CVSS 10.0 على خادم مشروع Alpine Linux



أعلن مشروع Alpine Linux عن محاولة استغلال الثغرة CVSS 10.0) CVE-2026-97229) على خادم GitLab الخاص به بعد أسبوع من إصدار الإصلاح، دون دليل على نجاحها.

- أعلن Alpine Linux في 28 أكتوبر أن مهاجماً حاول استغلال ثغرة حرجة في GitLab على خادمه الخاص.
- الثغرة هي CVE-2026-97229 بدرجة CVSS تبلغ 10.0.
- قد تتيح تنفيذ تعليمات برمجية على خادم GitLab عبر تعبير نمطي مصمم خصيصاً في إعدادات CI.
- جاءت المحاولة بعد أسبوع من إصدار GitLab للإصلاح.
- لم يجد Alpine دليلًا على نجاح الهجوم.

ما الذي حدث

أعلن مشروع Alpine Linux في 28 أكتوبر أن مهاجماً حاول استغلال ثغرة حرجة في GitLab على خادم GitLab الخاص بالمشروع. وقعت المحاولة بعد أسبوع من إصدار GitLab إصلاحاً للثغرة.

تحمل الثغرة الرمز CVE-2026-97229 ودرجة CVSS تبلغ 10.0. وبحسب التقرير، قد تتيح للمهاجم تنفيذ تعليمات برمجية على خادم GitLab عبر تعبير نمطي مصمم خصيصاً داخل إعدادات CI. ولم يجد Alpine دليلًا على نجاح الهجوم.

أهمية الخبر

تبيّن الحادثة أن محاولات استغلال الثغرات الحرجة قد تبدأ خلال أيام من نشر الإصلاح. وعلى الجهات التي تستضيف نسخ GitLab بنفسها، خاصة إذا كانت مسارات CI لديها تبني برمجيات داخلية أو تنشرها، أن تعدّ الفترة بين صدور الإصلاح وتثبيته فترة تعرّض فعلية.

لا يتضمن المصدر تفاصيل تقنية إضافية مثل الإصدارات المتأثرة أو أرقام الإصدارات المصححة، لذا ينبغي الرجوع إلى نشرة GitLab الرسمية.

الخطوات المقترحة

تحقّق مما إذا كانت جهتكم تشغّل GitLab مستضافاً ذاتياً، وراجعوا نشرة المورّد الخاصة بالثغرة CVE-2026-97229، وطبّقوا الإصلاح دون انتظار دورة التحديث الدورية. ثم افحصوا السجلات بحثاً عن تغييرات غير معتادة في إعدادات CI أو نشاط غير متوقع قرب وقت صدور الإصلاح.

ما يجب فعله الآن

1. حصر جميع نسخ GitLab المستضافة ذاتياً، بما فيها التي تستخدمها فرق التطوير وDevOps.
2. مراجعة نشرة GitLab الخاصة بالثغرة CVE-2026-97229 وتطبيق الإصلاح بصفة عاجلة.
3. فحص سجلات GitLab والخوادم بحثاً عن تغييرات غير معتادة في إعدادات CI أو نشاط غير متوقع.
4. تقليص إتاحة خوادم GitLab على الشبكة إلى الحد الضروري فقط.
5. تضمين مدد تطبيق التحديثات الحرجة لأدوات التطوير في إجراءات إدارة الثغرات.