GitLab تصدر تحديثات لثغرة تنفيذ تعليمات برمجية بأعلى درجات الخطورة CVE-2026-110264



أصدرت GitLab تحديثات لمعالجة الثغرة CVE-2026-110264 وهي فيض أعداد صحيحة بأعلى درجات الخطورة قد يتيح لمهاجم غير مصادق تنفيذ تعليمات برمجية على الخوادم. يُنصح بترقية النسخ فورًا.

- الثغرة CVE-2026-110264 هي فيض أعداد صحيحة في Regular Expression Compiler قد يسمح بتنفيذ تعليمات برمجية عن بُعد دون مصادقة.
- الإصلاح متوفر في إصدارات GitLab CE وEE التالية: 19.5.1 و19.4.3 و19.3.6 و19.2.9 و19.1.9 و19.0.10 و18.11.13.
- GitLab.com محدّثة بالفعل، ولا يلزم أي إجراء لعملاء GitLab Dedicated على internal0-19.3.5 أو internal0-19.4.2 أو أحدث.
- ترصد Shadowserver أكثر من 2,700 نسخة GitLab CE مكشوفة على الإنترنت دون بيان عدد المحدّث منها أو الأنظمة الوهمية.

- تأتي بعد ثغرة حرجة أخرى CVE-2026-97229 أُعلن عنها قبل عشرة أيام وأبلغ عنها الباحث نفسه.

أصدرت GitLab تحديثات أمنية لمعالجة الثغرة CVE-2026-110264 وهي ثغرة بأعلى درجات الخطورة قد تتيح لمهاجم عن بُعد وغير مصادق تنفيذ تعليمات برمجية على خادم ضعيف. وقد أبلغ عنها باحث يستخدم الاسم 'joaxcar' عبر برنامج مكافآت الثغرات لدى GitLab على منصة HackerOne.

طبيعة الثغرة

تتمثل المشكلة في فيض أعداد صحيحة داخل Regular Expression Compiler، وهو المحرك الذي يحلل ويتحقق من التعبيرات النمطية في ملفات الإعدادات. وفي ظروف معينة قد يؤدي تعبير نمطي مصمَّم خصيصًا إلى هذا الفيض ثم تنفيذ تعليمات برمجية على خادم GitLab.

عالجت GitLab الثغرة في إصدارات Community Edition وEnterprise Edition التالية: 19.5.1 و19.4.3 و19.3.6 و19.2.9 و19.1.9 و19.0.10 و18.11.13، وتحث المستخدمين على الترقية بأسرع وقت. أما GitLab.com فتعمل بالنسخة المصححة، وعملاء GitLab Dedicated على 19.3.5-0internal وinternal0-19.4.2 أو أحدث يتضمنون الإصلاحات بالفعل.

السياق الأوسع

ترصد Shadowserver أكثر من 2,700 نسخة من GitLab Community Edition مكشوفة على الإنترنت، دون توضيح عدد الأنظمة الوهمية أو التي جرى تأمينها. ولا يذكر المصدر استغلالاً فعليًا لهذه الثغرة تحديدًا.

وتأتي هذه الثغرة بعد CVE-2026-97229، وهي ثغرة حرجة أخرى لتنفيذ التعليمات عن بُعد في CI/CD Regular Expression Compiler أُعلن عنها قبل عشرة أيام وأبلغ عنها الباحث نفسه. وفي الشهر الماضي عالجت GitLab الثغرة CVE-2026-85706 التي تتيح لمهاجمين غير مصادقين قراءة بيانات حساسة، وأضافتها CISA في اليوم التالي إلى قائمة الثغرات المستغلة فعليًا. ومنذ نوفمبر 2021 أشارت CISA إلى خمس ثغرات في GitLab استُغلت في الهجمات.

وللجهات التي تدير GitLab ذاتيًا، تكمن الأولوية في التحقق من الإصدارات وتطبيق النسخة المصححة دون تأخير.

ما يجب فعله الآن

1. حصر جميع نسخ GitLab CE وEE المُدارة ذاتيًا والتحقق من إصداراتها مقارنة بالإصدارات المصححة.
2. ترقية النسخ المتأثرة إلى الإصدار المصحح للفرع المستخدم بأولوية، وقبل نوافذ التغيير الدورية متى سمحت السياسات.
3. التحقق من وجود نسخ GitLab يمكن الوصول إليها من الإنترنت، وتقييد الوصول إلى الشبكات الموثوقة أو VPN قدر الإمكان.
4. مراجعة سجلات الخوادم وCI/CD بحثًا عن نشاط غير معتاد، وتدوير بيانات الاعتماد والأسرار المخزنة في GitLab عند الاشتباه باختراق.
5. توثيق قرار التحديث وجدوله الزمني ضمن إدارة الثغرات والتحديثات وفق ضوابط الهيئة الوطنية للأمن السيبراني (NCA ECC) وإطار البنك المركزي السعودي (SAMA CSF).