أكثر من 1,000 خادم GitLab مكشوف على الإنترنت لا يزال دون ترقيع أمام ثغرة تنفيذ شيفرات عن بُعد مستغلة فعليًا



لا يزال أكثر من 1,000 خادم GitLab مكشوف على الإنترنت دون ترقيع أمام ثغرة بأعلى درجات الخطورة يستغلها المهاجمون فعليًا لتنفيذ شيفرات عن بُعد. على الجهات التي تشغّل GitLab التحقق من حالة الترقيع.

- لا يزال أكثر من 1,000 خادم GitLab مكشوف على الإنترنت دون ترقيع.
- الثغرة مصنّفة بأعلى درجات الخطورة.
- تُستغل الثغرة فعليًا في هجمات تنفيذ شيفرات عن بُعد (RCE).
- القاسم المشترك بين الخوادم المتأثرة هو إتاحتها على الإنترنت.

لا يزال أكثر من 1,000 خادم GitLab مكشوف على الإنترنت دون ترقيع أمام ثغرة بأعلى درجات الخطورة، بحسب BleepingComputer. وتُستغل الثغرة فعليًا في هجمات تتيح تنفيذ شيفرات عن بُعد (RCE).

أهمية الموضوع

يحتفظ GitLab عادةً بالشيفرة المصدرية ومسارات البناء وبيانات الاعتماد المستخدمة في نشر البرمجيات. لذلك قد يتحول الخادم الذي يتيح للمهاجم تنفيذ شيفرات عن بُعد إلى نقطة ارتكاز نحو بيئات التطوير والإنتاج. وبما أن الاستغلال جارٍ بالفعل، ينبغي التعامل مع النسخ المكشوفة وغير المرقّعة على أنها معرّضة للخطر الآن، لا في نافذة صيانة لاحقة.

ولا يتضمن المقتطع المتاح لنا تفاصيل تقنية إضافية، ولذلك لا يحدد هذا الخبر رقم الثغرة ولا الإصدارات المصححة. وعلى الفرق الرجوع إلى النشرة الأمنية الرسمية من الشركة المطورة.

الخطوات المقترحة

على الجهات التي تشغّل GitLab بنفسها التأكد سريعًا مما إذا كانت نسخها متاحة من الإنترنت، وهل طُبّق الإصلاح الصادر عن المورّد. وإذا تعذّر الترقيع فورًا، فإن تقليص الانكشاف خطوة مؤقتة معقولة. أما إذا كانت النسخة مكشوفة وغير مرقّعة، فمن الحكمة فحصها بحثًا عن مؤشرات اختراق وتدوير الأسرار المخزنة فيها.

كما يذكّر الأمر بضرورة إدراج بنية التطوير ضمن جرد الأصول وإدارة الثغرات والتغيير أسوةً بالأنظمة الحرجة الأخرى.

ما يجب فعله الآن

1. حصر جميع نسخ GitLab المُدارة ذاتيًا وتحديد المتاح منها من الإنترنت.
2. مراجعة النشرة الأمنية للمورّد وتطبيق الإصدار المصحَّح دون تأخير.
3. عند تعذر الترقيع الفوري، تقييد الوصول إلى النسخة (مثل VPN أو قوائم عناوين IP المسموحة).
4. فحص النسخ المكشوفة بحثًا عن مؤشرات اختراق مثل حسابات أو مهام أو سجلات وصول غير متوقعة.
5. تدوير الرموز والمفاتيح وبيانات الاعتماد المخزنة في أي نسخة كانت مكشوفة وغير مرقّعة.