GitLab تصدر إصلاحًا لثغرة تنفيذ أوامر عن بُعد بأعلى درجات الخطورة في الخوادم المستضافة ذاتيًا



أصدرت GitLab في 21 أكتوبر إصلاحات لثغرة بدرجة CVSS 10.0 تتيح لمهاجم دون مصادقة تنفيذ شيفرة على الخوادم المستضافة ذاتيًا، وتشمل كل الإصدارات منذ 7.0. ويلزم من حدّث في 12 أكتوبر أن يحدّث مجددًا.

- الثغرة بدرجة CVSS 10.0 وتتيح تنفيذ شيفرة على خادم GitLab مستضاف ذاتيًا دون تسجيل دخول.
- تشمل كل الإصدارات منذ الإصدار 7.0 الذي صدر عام 2014.
- نشرت GitLab الإصلاحات في 21 أكتوبر.
- غطّى تحديث 12 أكتوبر الإصدارات 19.2 فما فوق فقط.
- الإصدارات المصححة الجديدة أعلى بتحديث واحد من إصدار 12 أكتوبر، لذا لا يكفي التحديث السابق.

أصدرت GitLab إصلاحات لثغرة حرجة بدرجة CVSS 10.0، وهي الدرجة القصوى. وتتيح الثغرة لمهاجم تنفيذ شيفرة على خادم GitLab مستضاف ذاتيًا دون مصادقة. ووفق التقرير، تطال الثغرة كل إصدارات البرنامج منذ الإصدار 7.0 الذي صدر عام 2014.

لماذا قد لا يكفي التحديث السابق

نُشرت الإصلاحات في 21 أكتوبر. وعلى المسؤولين الذين طبّقوا تحديث 12 أكتوبر ألا يفترضوا أنهم محميون، فذلك التحديث غطّى الإصدارات 19.2 فما فوق فقط، والإصدارات المصححة الجديدة أعلى منه بتحديث واحد. وبالتالي ما زال على من حدّث قبل تسعة أيام الانتقال إلى الإصدار الجديد.

من المعرّض للخطر

تتعلق المسألة بالتثبيتات المستضافة ذاتيًا، حيث تتحمل المؤسسة نفسها مسؤولية تطبيق التحديثات. ولأن نطاق الإصدارات المتأثرة يمتد لأكثر من عقد، فإن النسخ القديمة التي نادرًا ما تُصان تدخل ضمن النطاق إلى جانب الحديثة. ولا يذكر المقتطف المتاح رقم CVE ولا دليلاً على الاستغلال ولا حلولاً مؤقتة، لذا ينبغي الرجوع إلى ملاحظات الإصدار الصادرة عن GitLab لهذه التفاصيل.

وغالبًا ما تحتوي مستودعات الشيفرة وخطوط CI/CD على بيانات اعتماد ومفاتيح نشر وشيفرة ملكية. ويمثل خلل تنفيذ الشيفرة دون مصادقة على خادم كهذا مصدر قلق جدي لأي جهة منظمة، ويستدعي معالجة سريعة ذات أولوية.

ما يجب فعله الآن

1. حصر جميع نسخ GitLab المستضافة ذاتيًا، بما فيها القديمة أو غير المصانة، وتوثيق إصداراتها.
2. ترقية كل نسخة إلى الإصدار المصحح الصادر في 21 أكتوبر حتى لو سبق تطبيق تحديث 12 أكتوبر.
3. التحقق من الإصدار المثبت بعد الترقية بدل الاكتفاء بتذكرة التغيير.
4. تقييد الوصول الشبكي إلى خوادم GitLab بنطاقات موثوقة إلى حين التأكد من اكتمال التحديث.
5. مراجعة سجلات الخوادم وخطوط الأتمتة بحثًا عن نشاط غير معتاد، وتدوير بيانات الاعتماد ومفاتيح النشر المخزنة في GitLab عند الاشتباه باختراق.
6. توثيق التحديث الطارئ في سجلات إدارة الثغرات والتغيير كدليل للتدقيق.