# CISA: ثغرة GitLab بأعلى درجات الخطورة تُستغل فعلياً في الهجمات



أفادت CISA بأن مهاجمين بدأوا باستغلال ثغرة في GitLab بأعلى درجات الخطورة، سبق إصلاحها مطلع هذا الشهر. على الجهات التي تدير GitLab بنفسها التحقق من حالة التحديث.

- تفيد CISA بأن ثغرة في GitLab بأعلى درجات الخطورة تُستغل الآن فعلياً.
- صدر الإصلاح الخاص بالثغرة مطلع هذا الشهر.
- الاستغلال الفعلي يعني أن الأنظمة غير المحدّثة معرّضة لخطر حقيقي لا نظري.
- المقتطف المتاح من المصدر لا يذكر رقم CVE ولا الإصدارات المتأثرة ولا تفاصيل الهجمات.

## ما الذي تم الإبلاغ عنه

ذكرت وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية (CISA) أن مهاجمين بدأوا باستغلال ثغرة في GitLab

مصنفة بأعلى مستويات الخطورة. وكانت الشركة المطورة قد أصدرت إصلاحاً للثغرة مطلع هذا الشهر، وبذلك انتقل الأمر من مهمة تحديث اعتيادية إلى تهديد قائم فعلياً.

النص المتاح من المصدر مختصر؛ فلا يذكر رقم CVE ولا الإصدارات المتأثرة ولا كيفية تنفيذ الهجمات أو الجهة التي تقف خلفها. لذا ينبغي الرجوع إلى نشرة الشركة المطورة وإشعار CISA للاطلاع على هذه التفاصيل قبل اتخاذ الإجراءات.

## أهمية الأمر

غالباً ما يحتفظ GitLab بالشيفرة المصدرية وخطوط CI/CD وبيانات الاعتماد وأسرار النشر. لذلك قد يكشف اختراق أي نسخة منه أكثر بكثير من المنصة نفسها. وبعد تأكيد الاستغلال الفعلي، تلاشت المهلة بين صدور الإصلاح وبدء الهجمات، ويجب التعامل مع أي نسخة غير محدّثة بوصفها تعرضاً ذا أولوية.

## الخطوات التالية

على الجهات التي تدير GitLab بنفسها أن تتحقق سريعاً مما إذا كانت على إصدار مُصلَح، وهل النسخة متاحة من الإنترنت. وإن تعذّر التحديث فوراً، فمن المناسب تقليص التعرض ومراجعة السجلات بحثاً عن نشاط غير معتاد كإجراء مؤقت. ويُنصح بتوثيق نتائج هذه الفحوصات، إذ تتوقع الجهات التنظيمية دليلًا على إدارة الثغرات في الوقت المناسب للأنظمة الحرجة.

## ما يجب فعله الآن

1. حصر جميع نسخ GitLab المُدارة ذاتياً والتأكد من أن كل نسخة تعمل بإصدار يتضمن إصلاح الشركة المطورة.
2. تطبيق التحديث فوراً على أي نسخة لم تُحدَّث بعد، مع البدء بالنسخ المتاحة من الإنترنت.
3. تقييد الوصول الخارجي إلى النسخ غير المحدّثة إلى حين اكتمال التحديث.
4. مراجعة سجلات الوصول والنظام في GitLab بحثاً عن نشاط غير معتاد منذ صدور الإصلاح، ورفع أي ملاحظات إلى فريق الاستجابة للحوادث.
5. تدوير بيانات الاعتماد والرموز وأسرار خطوط النشر المخزنة في أي نسخة ربما تعرضت للخطر.
6. توثيق حالة التحديث ونتائج المراجعة كدليل على الالتزام بمتطلبات إدارة الثغرات.