بيانات اعتماد مسرّبة تبقى صالحة سنوات بسبب الخشية مما قد يتعطل عند إلغائها



وجد تقرير GitGuardian لعام 2026 أن أكثر من 64% من الأسرار الصالحة المكتشفة في 2022 ظلت تعمل في يناير 2026، لأن الفرق تتردد خشية تعطل الأنظمة عند الإلغاء.

- بحسب تقرير GitGuardian لعام 2026، ظل أكثر من 64% من الأسرار الصالحة المكتشفة في 2022 صالحًا في يناير 2026.
- تتأخر الفرق في المعالجة لأنها لا تعرف ما الذي سيتعطل عند الإلغاء.
- الفرز المبني على صلاحية السر وحدها يفوّت 46% من الأسرار الحرجة.
- يوصي المصدر بالفرز حسب الأثر: ما الذي يستطيع الاعتماد الوصول إليه، وهل سُرّب علنًا.

ما الذي كشفه التقرير

يفيد تقرير GitGuardian لعام 2026 (State of Secrets Sprawl) بأن معظم الأسرار الصالحة التي اكتُشفت في 2022 كانت لا تزال تعمل في يناير 2026، إذ بقي أكثر من 64% منها صالحًا بعد أربع سنوات. والسبب المذكور ليس ضعف الاكتشاف، بل التردد: تتوقف الفرق لأنها لا تعرف ما الذي سيتعطل عند إلغاء الاعتماد.

لماذا لا يكفي معيار الصلاحية

يشير المصدر إلى أن الفرز القائم على صلاحية السر فقط يفوّت 46% من الأسرار الحرجة. ويوصي بالترتيب حسب الأثر، أي النظر في ما يمكن للاعتماد الوصول إليه وفي ما إذا كان قد انكشف علنًا. أما بقية نص المصدر، ومنها المادة عن انكشاف الهويات ومسارات الهجوم، فهي محتوى ترويجي مقتضب دون تفاصيل إضافية.

الدلالة للجهات المنظمة

بالنسبة لقادة المخاطر والامتثال، فإن بقاء اعتماد مكشوف مدة طويلة يعكس غالبًا غياب خريطة للتبعيات. فإذا لم يعرف أحد أي الخدمات تعتمد على سر معين، تأخر الإلغاء واستمر التعرض. وبناء هذه المعرفة قبل وقوع الحادث يجعل المعالجة أسرع وأقل تعطيلاً للأعمال.

ما يجب فعله الآن

1. الاحتفاظ بسجل للأسرار ومفاتيح الواجهات البرمجية مع تحديد المالك والخدمات المعتمدة عليها.
2. ترتيب الاعتمادات المكشوفة حسب ما تصل إليه وحسب تسريبها علنًا، لا حسب صلاحيتها فقط.
3. اعتماد إجراء مُختبر لتدوير الأسرار مع خطة تراجع حتى لا يقوم الإلغاء على التخمين.
4. تحديد مهل مستهدفة لإلغاء الأسرار المكشوفة ومتابعة المتأخر منها حتى الإغلاق.
5. مراجعة نتائج الفحص القديمة للأسرار التي لم تُعالج بعد.