حملة «wfx-loot» تستغل نحو 4,800 حساب GitHub مخترق لسرقة أسرار CI وبيانات السحابة



رصدت Aikido حملة استخدمت 4,837 حساب GitHub مخترقاً لفحص 61,764 مستودعاً وسرقة أسرار Actions وبيانات السحابة، وقد سُرقت أسرار من 1,835 هدفاً على الأقل.

- بدأت الحملة نحو الساعة 12:45 بالتوقيت العالمي في 10 نوفمبر، باستخدام بيانات اعتماد مسروقة من 4,837 حساباً لاختبار صلاحية الكتابة على 61,764 مستودعاً.
- نُشرت طلبات سحب بعنوان «docs: dependency audit notes» تحمل سكربت شل من نحو 1,500 سطر، ولا يزال 92% منها مفتوحاً.
- يجمع السكربت رموز GitHub وبيانات AWS وAzure وGoogle Cloud ومفاتيح المطورين وخدمات الذكاء الاصطناعي، ويستطيع استبدال رموز OIDC بجلسات سحابية مؤقتة.
- أكدت Aikido سرقة أسرار من 1,835 هدفاً على الأقل، كما وصلت الشيفرة الخبيثة إلى حزمة Packagist وإصدارين من وحدة Go عبر النشر الآلي.

- عند تأكيد التنفيذ، تُعدّ جميع الأسرار والأدوار السحابية المتاحة لمسارات العمل المتأثرة مخترقة وتجب إعادة تدويرها.

وصف باحثو Aikido حملة باسم «wfx-loot» تستهدف أسرار GitHub Actions وبيانات اعتماد السحابة. ورغم أن الحمولة لم تُنفَّذ في كل مستودع مستهدف، فقد سُرقت أسرار من 1,835 هدفاً على الأقل.

كيف نُفِّذ الهجوم

وفق Aikido، استخدم المهاجم بيانات اعتماد مسروقة من 4,837 حساباً مخترقاً لفتح طلبات سحب على 61,764 مستودعاً بهدف اختبار صلاحية الكتابة. حملت الطلبات عنوان «docs: dependency audit notes». وتشير التقارير إلى أن بعض الحسابات تعود إلى جهات كبرى وحكومية، وأن نحو 50 منها يبدو أنها تملك صلاحيات نشر على منظومات مثل npm وPyPI وGo وcrates وPackagist.

وحيثما سمحت الصلاحيات، سُلّم سكربت شل من نحو 1,500 سطر عبر تعديل مسار عمل قائم، أو إضافة مسار جديد على فرع قصير العمر، أو زرع خطاف npm install. يجمع السكربت رموز مسارات العمل وبيانات اعتماد AWS وAzure وGoogle Cloud وبيانات أدوات مثل Git وSSH وDocker وKubernetes وVault وTerraform ومفاتيح خدمات الذكاء الاصطناعي. ويمكنه أيضاً استبدال رموز OIDC بجلسات سحابية مؤقتة، وإنشاء بيانات اعتماد طويلة الأمد أو تعديل سياسات الهوية والثقة متى سمحت الصلاحيات. أُرسلت البيانات إلى نقطتين يتحكم بهما المهاجم، وحُذفت التغييرات وسجلات التشغيل في أقل من دقيقة.

ما الذي ينبغي على المالكين فحصه

تنصح Aikido مالكي المستودعات بالبحث عن فرع «wfx-docs» وطلب السحب الاستكشافي وفجوات في أرقام تشغيل مسارات العمل. وعند تأكيد التنفيذ، تُعدّ جميع الأسرار والأدوار السحابية المتاحة لمسارات العمل المتأثرة مخترقة وتجب إعادة تدويرها فوراً. ويرجّح الباحثون أن الهدف الرئيسي كان سرقة أسرار CI، وأن إصدارات الحزم جاءت نتيجة جانبية للنشر الآلي.

ما يجب فعله الآن

1. ابحثوا في مستودعات GitHub عن فرع «wfx-docs» وطلبات السحب بعنوان «docs: dependency audit notes» وأي فجوات غير مفسرة في أرقام تشغيل مسارات العمل.
2. عند تأكيد تنفيذ الحمولة، أعيدوا تدوير جميع الأسرار والأدوار السحابية المتاحة لمسارات العمل المتأثرة فوراً، بما فيها مفاتيح AWS وAzure وGCP والسجلات وخدمات الذكاء الاصطناعي.
3. راجعوا سجلات التدقيق السحابية بحثاً عن بيانات اعتماد IAM طويلة الأمد جديدة أو ربط أدوار أو تغييرات في سياسات الهوية والثقة صادرة عن هويات CI.
4. تحققوا مما إذا كانت حزمكم أو وحداتكم قد نُشرت آلياً من مسارات عمل متأثرة، وراجعوا سلامة الإصدارات الأخيرة.
5. قيّدوا صلاحيات الكتابة وأذونات Actions بالحد الأدنى اللازم، وفرضوا المصادقة متعددة العوامل وسلامة بيانات الاعتماد لحسابات المطورين.