اختراق حزمة Microsoft Agent Framework على PyPI لسرقة بيانات اعتماد السحابة



أفادت جهات بحثية باختراق حزمة agent-framework من Microsoft. الإصدارتان 1.26.1 و1.26.2، المنشوران في 17 نوفمبر 2026، تشغّلان أداة سرقة بيانات اعتماد عند كل تشغيل لبايثون.

- نُشرت النسختان الخبيثتان 1.26.1 و1.26.2 من حزمة agent-framework على PyPI بفارق 33 دقيقة في 17 نوفمبر 2026.
- صُمّم الكود لتشغيل أداة سرقة بيانات اعتماد عند كل تشغيل لبايثون.
- أبلغت عن الحادثة عدة شركات أمنية منها Aikido وChainguard وEndor Labs وOX Security وSafeDep وSocket وStepSecurity وWiz.
- الهدف المعلن هو سرقة بيانات اعتماد السحابة.

ما الذي حدث

تفيد عدة شركات أمنية بأن حزمة agent-framework التابعة لـ Microsoft على PyPI تعرضت للاختراق واستُخدمت لتوزيع أداة سرقة بيانات اعتماد. نُشر إصداران خبيثان، هما 1.26.1 و1.26.2، بفارق 33 دقيقة في 17 نوفمبر 2026.

لماذا يهم ذلك

وفق التقارير، صُممت الإصدارات الخبيثة لتشغيل أداة السرقة عند كل بدء لبايثون. وهذا يعني أن مجرد وجود إصدار متأثر في بيئة ما قد يكفي لتنفيذ الكود، دون استدعاء الحزمة مباشرة. والهدف المعلن هو سرقة بيانات اعتماد السحابة، وهو ما قد يمنح المهاجم وصولًا إلى الحسابات السحابية والبيانات وأحمال العمل المرتبطة بها.

لا يوضح المقتطف المتاح كيف جرى الحصول على صلاحية النشر، ولا المدة التي بقيت فيها الإصدارات متاحة، ولا عدد البيئات المتأثرة. لذا ينبغي ألا تفترض المؤسسات أنها متأثرة أو سليمة قبل فحص بيئاتها.

الخطوات التالية

تعامل مع الحادثة بوصفها حادثة في سلسلة توريد البرمجيات. تحقق مما إذا كان الإصدار 1.26.1 أو 1.26.2 قد ثُبّت في أي مكان، بما في ذلك أجهزة المطورين وخطوط البناء والحاويات ودفاتر العمل السحابية. وعند وجودهما، افترض أن أي بيانات اعتماد يمكن الوصول إليها من تلك البيئة قد تكون مكشوفة وقم بتدويرها. وتابع الإرشادات الصادرة عن الشركات المذكورة وعن Microsoft مع تطور الحادثة.

ما يجب فعله الآن

1. ابحث في جميع بيئات بايثون وخطوط البناء والحاويات وملفات القفل عن الإصدارين 1.26.1 و1.26.2 من agent-framework.
2. عند وجود أي من الإصدارين، دوّر بيانات اعتماد السحابة والرموز والأسرار التي يمكن الوصول إليها من تلك البيئة.
3. راجع سجلات التدقيق السحابية بحثاً عن تسجيلات دخول أو نشاط واجهات برمجية غير معتاد من الهويات المتأثرة.
4. ثبّت إصدارات الاعتمادات واستخدم مستودعاً داخلياً للحزم أو خطوة موافقة قبل اعتماد الإصدارات الجديدة.
5. وثّق الحادثة ضمن عملية إدارة مخاطر الأطراف الخارجية وسلسلة التوريد وأبلغ فريق عمليات الأمن.