SAP تؤكد وقوع حادث أمني مرتبط بنشاط مشبوه على GitHub



أكدت SAP رصد نشاط مشبوه واتخاذ إجراءات لحماية عملائها، دون دليل حتى الآن على وصول غير مصرح به إلى بيانات العملاء. وتتحدث تقارير صحفية عن سرقة رموز مصادقة وتعديل شيفرة على GitHub.

- أكدت SAP أنها رصدت نشاطاً مشبوهاً في بيئتها التقنية واتخذت إجراءات وقائية.
- تفيد الشركة بعدم وجود دليل حتى الآن على وصول غير مصرح به إلى بيانات أعمال العملاء.
- نقلت Der Spiegel عن مذكرة داخلية أن الهجوم يُعرف داخلياً باسم "Project Granite"، وأن المهاجمين سرقوا رموز مصادقة للموظفين ونسخوا شيفرة مصدرية على GitHub وعدّلوها.
- لم توضح SAP البيئات المتأثرة ولا ما إذا كان على العملاء الذين يستخدمون شيفرة من مستودعاتها على GitHub اتخاذ إجراء.
- حذّر مكتب BSI الألماني بشكل منفصل من أدوات ذكاء اصطناعي وكيلية تيسّر الهجمات

السيبرانية.

أكدت SAP لموقع BleepingComputer أنها رصدت نشاطاً مشبوهاً في بيئتها التقنية وتحركت سريعاً لحماية عملائها. وتقول الشركة إن تحقيقها حتى الآن لم يجد دليلًا على وصول غير مصرح به إلى بيانات أعمال العملاء.

ما الذي نُشر

نقلت Der Spiegel عن مذكرة داخلية في SAP أن الشركة تتعامل مع هجوم يحمل الاسم الرمزي "Project Granite". ووفق مصادر الصحيفة، اخترق المهاجمون بيئة GitHub الخاصة بالشركة، وربما بمساعدة أدوات ذكاء اصطناعي. ويُقال إنهم سرقوا رموز مصادقة تخص موظفين واستخدموها لنسخ الشيفرة المصدرية وتعديلها. ولم تؤكد SAP هذه التفاصيل التقنية.

ما لم يتضح بعد

لم تحدد SAP البيئات المتأثرة، ولم توضح ما إذا كان على العملاء الذين يحمّلون شيفرة من مستودعاتها على GitHub، أو يتلقون تحديثات تُجلب منها بشكل مباشر أو غير مباشر، اتخاذ أي إجراء. وامتنع متحدث باسم الشركة عن تقديم مزيد من المعلومات.

وفي سياق منفصل، حذّر المكتب الاتحادي الألماني لأمن المعلومات (BSI) مؤخراً من أدوات ذكاء اصطناعي وكيلية تعزز قدرات الهجمات السيبرانية، ودعا المؤسسات إلى التركيز على الاستجابة للحوادث وتطبيق ممارسات التحصين الموصى بها.

قراءة عملية

لا يوجد حتى الآن أثر مؤكد على العملاء. والمسار الأنسب للمؤسسات التي تشغّل SAP هو التعامل بهدوء، وحصر مكونات SAP والمستودعات التي تعتمد عليها فرقها، ومتابعة إفادات الشركة مع تطور التحقيق.

ما يجب فعله الآن

1. احصر منتجات SAP والإضافات والشيفرة أو الحزم المستضافة على GitHub التي تستخدمها فرقكم أو تجلب منها تحديثات.
2. اطلبوا من مدير حساب SAP إفادة مكتوبة عمّا إذا كانت أي مستودعات أو قنوات تحديث متأثرة.
3. تحققوا من سلامة ومصدر أي شيفرة أو حزم من SAP جُلبت مؤخراً من GitHub قبل نشرها.
4. راجعوا حسابات GitHub وحسابات المطورين لديكم: دوّروا الرموز طويلة الأمد، وفعّلوا المصادقة متعددة العوامل، وطبقوا أقل الصلاحيات.
5. سجّلوا الحدث في سجل مخاطر الأطراف الخارجية وأطلعوا مسؤول أمن المعلومات، بما يتسق مع متطلبات الأطراف الخارجية في ضوابط NCA ECC وإطار SAMA CSF.
6. تأكدوا من أن خطط الاستجابة للحوادث تغطي الحوادث الصادرة عن الموردين وسرقة رموز المصادقة.