استغلال ثغرة في Azure API Management ضد شركتي طاقة نرويجيتين



أفادت هيئة الأمن الوطني النرويجية بأن جهة مجهولة استغلت ثغرة في فئات قديمة من Azure API Management لاستهداف رموز الوصول، وتأثرت Equinor وSkagerak Energi. أصلحت Microsoft الخلل ونشرت إرشادات لاستبدال بيانات الاعتماد المكشوفة.

- أثرت الثغرة في Azure API Management، واستهدفت جهة مجهولة رموز الوصول وبيانات حساسة أخرى مخزّنة فيه.
- رصدت Equinor الهجوم يوم الثلاثاء واحتوته بالكامل يوم الجمعة، واستمر إنتاج النفط والغاز دون مؤشر على سرقة بيانات.
- أبلغت Skagerak Energi عن هجوم منفصل لم يؤثر في عملياتها أو إنتاج الكهرباء.
- تقول Microsoft إنها اكتشفت المشكلة في 18 نوفمبر وأغلقت مسار الوصول في اليوم التالي، وإن الإصدارات الأحدث من APIM لم تتأثر.

- كان المتضررون في الغالب عملاء خزّنوا أسرارًا مباشرة في APIM بدل Azure Key Vault.

أعلنت هيئة الأمن الوطني النرويجية (NSM) أن شركتي Equinor وSkagerak Energi من بين الجهات المتأثرة بثغرة في خدمة Azure API Management (APIM) من Microsoft، وهي خدمة تُستخدم لإدارة الاتصالات بين التطبيقات والأنظمة الأخرى وتأمينها. ووفق الهيئة، تستهدف جهة تهديد مجهولة بشكل نشط رموز الوصول وغيرها من المعلومات الحساسة المخزّنة في المنصة.

ما المعروف حتى الآن

ذكرت Equinor أنها رصدت الهجوم يوم الثلاثاء واحتوته بالكامل يوم الجمعة. تعطلت بعض الخدمات الداخلية، لكن إنتاج النفط والغاز استمر بصورة طبيعية. وقالت الشركة إنه لا يوجد ما يشير إلى سرقة البيانات أو تعديلها، وإن الهجوم لم يبدُ موجّهًا إليها تحديدًا. أما Skagerak Energi فأعلنت عن هجوم منفصل، وأكدت أن عملياتها وإنتاج الكهرباء لم يتأثرا.

وبحسب ما ورد، أبلغت Microsoft عملاءها في إشعار غير علني بأنها اكتشفت في 18 نوفمبر مشكلة أمنية في الفئات القديمة "Classic" من APIM وأغلقت مسار الوصول في اليوم التالي. وحذّرت من أن كلمات مرور وأسرارًا أخرى مخزّنة في الأنظمة المعرّضة ربما جرى الوصول إليها قبل ذلك. وأفادت لاحقًا لـ Recorded Future News بأن عدة فئات، منها Developer وBasic وStandard وPremium، تأثرت وتم إصلاحها. ولم تذكر عدد العملاء المكشوفين ولا ما إذا كانت جهة واحدة وراء جميع الحوادث.

أهمية الأمر

قالت NSM إنه من غير الواضح مدى استغلال الثغرة سابقًا أو حاليًا، وحذّرت من أن جهات أخرى قد تحاول استغلالها بعد الإعلان عنها. وارتبط التعرض في الغالب بعملاء لم يتبعوا توصيات Microsoft أو خزّنوا بيانات حساسة مباشرة في APIM بدل Azure Key Vault.

على الجهات في المملكة التي تستخدم APIM، وخصوصًا في قطاع الطاقة والقطاعات الحيوية، مراجعة تعرّضها واعتبار أي سر مخزّن فيه مكشوفًا محتملاً إلى حين التحقق.

ما يجب فعله الآن

1. حصر جميع نسخ Azure API Management لديكم، بما فيها فئات Classic وDeveloper وBasic وStandard وPremium.
2. تطبيق إرشادات Microsoft المنشورة لتحديد بيانات الاعتماد والرموز وكلمات المرور المحتمل كشفها واستبدالها.
3. نقل الأسرار المخزّنة مباشرة في APIM إلى Azure Key Vault ومواءمة الإعدادات مع توصيات Microsoft الأمنية.
4. مراجعة سجلات APIM والهوية ذات الصلة بحثًا عن استخدام غير معتاد للرموز أو وصول مريب منذ منتصف نوفمبر.
5. إدراج الحادثة في إجراءات الاستجابة وإدارة مخاطر الأطراف الثالثة، وإحاطة فرق التقنية التشغيلية والطاقة عند الاقتضاء.