مايكروسوفت تعالج ثغرة في Azure API Management وسط استهداف مهاجم لأسرار العملاء



أفادت هيئة الأمن الوطني النرويجية بأن ثغرة في Azure API Management أثّرت على عدة جهات نرويجية، منها Skagerak Energig Equinor، وأن مهاجماً مجهولًا بحث عن رموز الوصول والأسرار. وقد عالجت مايكروسوفت الثغرة.

- كشفت هيئة الأمن الوطني النرويجية (NSM) عن ثغرة في خدمة Azure API Management من مايكروسوفت.
- تأثرت عدة جهات في النرويج، ومنها شركتا الطاقة Skagerak Energig Equinor.
- كان مهاجم مجهول يبحث بنشاط عن رموز الوصول والأسرار والقيم المسماة (named values) في APIM.
- وفق عنوان الخبر، عالجت مايكروسوفت الثغرة.
- لا يقدّم المقتطف المتاح تفاصيل تقنية ولا حجم الأثر الكامل.

أعلنت هيئة الأمن الوطني النرويجية (NSM) أنها علمت بثغرة في خدمة Azure API Management (APIM) من مايكروسوفت أثّرت على عدة جهات في البلاد، من بينها شركتا الطاقة Equinor وSkagerak Energi.

ما المعروف حتى الآن

وفق الهيئة، كان مهاجم مجهول يبحث بنشاط داخل APIM عن رموز الوصول والأسرار والقيم المسماة (named values). وهذه عناصر قد تفتح الطريق إلى أنظمة وبيانات مرتبطة بها. ويشير عنوان الخبر إلى أن مايكروسوفت عالجت الثغرة التي تخص الفئة الكلاسيكية من الخدمة.

لا يوضح المقتطف المتاح لنا آلية عمل الثغرة، ولا عدد الجهات المتأثرة، ولا ما إذا أُسيء استخدام أي بيانات. لذلك لم نبنِ استنتاجات في هذه النقاط.

أهمية الأمر للمؤسسات في المملكة

أي جهة تستخدم APIM لنشر واجهات البرمجة أو حمايتها قد تحتفظ داخل الخدمة بمعلومات اعتماد وقيم إعداد حساسة. وإذا كشفت ثغرة على مستوى المنصة هذه القيم، فإن الخطر يمتد إلى كل نظام تتيح الوصول إليه. وينبغي لمشغّلي قطاع الطاقة والقطاعات الحيوية الأخرى في المملكة اعتبار الخبر دافعاً لمراجعة طريقة تخزين الأسرار وتدويرها في بوابات الواجهات البرمجية.

المناسب هنا مراجعة هادئة ومنهجية: تأكيد التعرض، وفحص أي نشاط غير معتاد، وتدوير القيم الحساسة عند أي شك، مع متابعة إرشادات مايكروسوفت وNSM كلما صدرت تفاصيل إضافية.

ما يجب فعله الآن

1. حصر جميع نسخ Azure API Management، بما فيها الفئة الكلاسيكية، والتأكد من تطبيق معالجات مايكروسوفت.
2. جرد رموز الوصول والأسرار والقيم المسماة المخزنة في APIM وتدوير ما لا يمكن استبعاد تعرضه.
3. نقل القيم الحساسة إلى مخزن أسرار مخصص بصلاحيات مقيدة متى أمكن.
4. مراجعة سجلات APIM وAzure بحثاً عن قراءة غير معتادة للأسرار أو قيم الإعداد.
5. إدراج منصات بوابات الواجهات البرمجية ضمن مراجعات مخاطر الأطراف الخارجية والخدمات السحابية بما يتوافق مع ضوابط NCA ECC وNCA CCC.