استغلال ثغرة في طبقات Azure API Management Classic لسرقة بيانات اعتماد واجهات البرمجة المخزنة



حذّرت مايكروسوفت من استغلال ثغرة في طبقات Azure API Management (APIM) Classic لسرقة بيانات اعتماد واجهات البرمجة المخزنة، وربطت جهات نرويجية الثغرة بهجمات على شركات طاقة.

- تحذّر مايكروسوفت عملاءها من ثغرة في طبقات Azure API Management (APIM) Classic.
- استُغلت الثغرة لسرقة بيانات اعتماد واجهات البرمجة المخزنة في الخدمة.
- ربطت جهات نرويجية الثغرة بهجمات إلكترونية استهدفت شركات طاقة.
- لا يتضمن المقتطف المتاح رقم CVE أو تفاصيل الإصلاح أو عدد العملاء المتأثرين.

أبلغت مايكروسوفت عملاءها بأن ثغرة أمنية في طبقات Classic من خدمة Azure API Management (APIM) استُغلت في هجمات فعلية لسرقة بيانات اعتماد واجهات البرمجة المخزنة في الخدمة. كما ربطت جهات نرويجية

هذه الثغرة بهجمات إلكترونية استهدفت شركات طاقة.

ما المعروف حتى الآن

المقتطف المتاح من التقرير موجز. فهو يحدد المكوّن المتأثر (طبقات APIM Classic) والأثر (سرقة بيانات اعتماد واجهات البرمجة المخزنة) وربط الجهات النرويجية الثغرة بهجمات على قطاع الطاقة. ولا يذكر رقم CVE ولا وصفاً تقنياً ولا فترة الاستغلال ولا عدد الجهات المتأثرة، ولذلك لا ينبغي افتراض أي منها.

أهمية الخبر

غالباً ما تمنح بيانات اعتماد واجهات البرمجة وصولًا إلى الأنظمة الخلفية وتكاملات الشركاء وخدمات البيانات. وإذا انكشفت، فقد يتمكن المهاجم من استخدامها دون تفعيل ضوابط تسجيل الدخول المعتادة. لذا يجدر بالمؤسسات التي تستخدم طبقات APIM Classic التعامل مع الأمر بوصفه حالة محتملة لانكشاف بيانات اعتماد، لا مجرد مهمة تحديث.

ويهمّ استهداف قطاع الطاقة المشغّلين السعوديين للبنى التحتية الحرجة، والمؤسسات المالية التي تعتمد على الخدمة السحابية نفسها.

النهج المقترح

تحقق مما إذا كانت مؤسستك تستخدم طبقات APIM Classic، واتبع إرشادات مايكروسوفت للعملاء، وراجع بيانات الاعتماد المخزنة في الخدمة. ويُرجع إلى إشعار مايكروسوفت نفسه للتفاصيل الكاملة لأن المقتطف المتاح محدود.

ما يجب فعله الآن

1. حدّد جميع نسخ Azure API Management العاملة على طبقات Classic ضمن اشتراكاتكم.
2. راجع إشعار مايكروسوفت للعملاء وطبّق إرشادات المعالجة الواردة فيه.
3. بدّل مفاتيح واجهات البرمجة والأسرار وبيانات الاعتماد المخزنة في نسخ APIM المتأثرة أو المُدارة عبرها.
4. راجع سجلات الوصول إلى واجهات البرمجة والأنظمة الخلفية بحثاً عن استخدام غير متوقع لهذه البيانات.
5. أطلع رئيس أمن المعلومات، وأبلغ الجهة التنظيمية أو القطاعية عند الاقتضاء وفق متطلبات الإبلاغ عن الحوادث.