ثغرة في Azure API Management كشفت أسرارًا وأثّرت على شركات طاقة نرويجية



تُبلغ مايكروسوفت عملاءها بثغرة في Azure API Management Classic قد تكشف أسرارًا مخزنة. وتربطها هيئة الأمن الوطني النرويجية بحوادث في Equinor Energig Skagerak وتنصح بعدّ الأسرار مخترقة.

- اكتشفت مايكروسوفت المشكلة في Azure API Management (APIM) في 18 نوفمبر وأغلقت مسار الوصول في اليوم التالي.
- قد تشمل البيانات المكشوفة القيم المسماة وأسرار العميل لمزوّدي الهوية ومفاتيح الاشتراك ورموز واجهات الإدارة المباشرة.
- النسخ Classic من APIM التي لا تتبع إرشادات الأمان الموثقة من مايكروسوفت متأثرة، بينما لا تتأثر طبقات v2.
- تفيد هيئة الأمن الوطني النرويجية (NSM) بأن عدة جهات تضررت ومنها Equinor وSkageraks

Energi، وأن قطاعات أخرى داخل النرويج وخارجها متأثرة.

- حجم الاستغلال الفعلي غير واضح.

ما الذي حدث

تُبلغ مايكروسوفت عملاءها بمشكلة أمنية في خدمة Azure API Management (APIM) المستخدمة لنشر واجهات البرمجة وحمايتها وإدارتها. ووفق إشعار عميل جرى تداوله علنًا، حددت مايكروسوفت المشكلة في 18 نوفمبر وأغلقت مسار الوصول في اليوم التالي. وتذكر الشركة أنه كان بإمكان طرف غير مصرح له استغلال الثغرة للوصول إلى أسرار مخزنة في نسخ APIM Classic قبل اكتشافها.

وذكرت هيئة الأمن الوطني النرويجية (NSM) في 20 نوفمبر أن الثغرة أثرت على عدة جهات في البلاد، منها شركتا الطاقة Equinor وSkagerak Energig اللتان أعلنتا كلٌّ على حدة عن حوادث في الأسبوع السابق. وأفادت Equinor بعدم وجود دليل على سرقة البيانات أو تعديلها، وقالت Skagerak Energi إن العمليات والإنتاج لم تتأثر ولم تجد دليلاً على المساس بالمعلومات.

من المعرّض للخطر

تتعلق المشكلة بطبقات APIM Classic التي لا تلتزم بإرشادات الأمان الموثقة من مايكروسوفت، أما طبقات v2 فغير متأثرة. وتشمل البيانات المعرضة القيم المسماة وأسرار العميل لمزوّدي الهوية ومفاتيح الاشتراك ورموز واجهات الإدارة المباشرة. وتقول NSM إن جهة مجهولة استهدفت الرموز والأسرار والقيم المسماة، وإن عدة قطاعات داخل النرويج وخارجها متأثرة، ولا يزال مدى الاستغلال غير واضح.

وحذّر الخبير Anders Kristiansen من أن بيانات الاعتماد المسحوبة من APIM قد تُستخدم ضد خدمات خارجية، ويتوقف حجم الضرر على صلاحيات كل بيان اعتماد.

ما توصي به NSM

على مستخدمي APIM عدّ أسرارهم وقيمهم المسماة مخترقة واستبدالها، والتأكد من تحديث نسخهم، وتحديد البيانات التي يمكن الوصول إليها عبر الخدمة.

ما يجب فعله الآن

1. حصر نسخ Azure APIM وتحديد ما يعمل منها على طبقات Classic، بما فيها ما يديره الموردون نيابة عنكم.
2. عدّ جميع القيم المسماة وأسرار العميل لمزوّدي الهوية ومفاتيح الاشتراك ورموز واجهات الإدارة في نسخ Classic مخترقة وتدويرها.
3. التحقق من إشعار مايكروسوفت ومن بيئتكم أن النسخ محدّثة وتتبع إرشادات الأمان الموثقة.
4. تحديد الأنظمة الخلفية والخدمات الخارجية التي يصل إليها كل بيان اعتماد في APIM ومراجعة سجلاتها بحثًا عن وصول غير معتاد.
5. إذا كانت APIM تدعم خدمات حرجة أو مرتبطة بالتقنيات التشغيلية، فأبلغوا عن أي اشتباه بالتعرض عبر مسار إدارة الحوادث ولدى الجهات المعنية مثل الهيئة الوطنية للأمن السيبراني والجهة التنظيمية

القطاعية عند الاقتضاء.