Azure API Management flaw exploited against Norwegian energy firms



Norway's NSM says an unidentified actor exploited a flaw in older Azure API Management tiers to target access tokens, affecting Equinor and Skagerak Energi. Microsoft has fixed the issue and published guidance on replacing exposed credentials.

- The flaw affected Azure API Management, and an unidentified actor targeted access tokens and other sensitive data stored in it.
- Equinor detected its attack on a Tuesday and contained it by Friday; oil and gas production continued and no data theft was indicated.
- Skagerak Energi reported a separate attack with no impact on operations or power production.
- Microsoft says it found the issue on November 18, closed the access path the next day, and that newer APIM versions were not affected.

> - Customers who stored secrets directly in APIM rather than Azure Key Vault were mainly exposed.

Norway's National Security Authority (NSM) has said that Equinor and Skagerak Energi are among the organizations affected by a vulnerability in Microsoft's Azure API Management (APIM), a service used to manage and secure connections between applications and other systems. According to NSM, an unidentified threat actor has been actively targeting access tokens and other sensitive information stored in the platform.

What is known

Equinor said it detected the attack on a Tuesday and fully contained it by Friday. Some internal services were disrupted, but oil and gas production continued normally. The company said there was no indication that data was stolen or altered, and that it did not appear to have been specifically targeted. Skagerak Energi disclosed a separate attack and said operations and power production were unaffected.

Microsoft reportedly told customers in a non-public advisory that it found a security issue in the older "Classic" tiers of APIM on November 18 and closed the access path the next day. It warned that passwords and other secrets stored in vulnerable instances may have been accessed beforehand. Microsoft later told Recorded Future News that several tiers, including Developer, Basic, Standard and Premium, were affected and fixed. It has not said how many customers were exposed or whether one actor is behind all incidents.

Why it matters

NSM said it is unclear how widely the flaw has been or is being exploited, and warned that other actors may try to exploit it now that it is public. The exposure was mainly linked to customers who had not followed Microsoft's recommendations or who kept sensitive data directly in APIM instead of Azure Key Vault.

Organizations in Saudi Arabia that use APIM, particularly in energy and other critical sectors, should check their exposure and treat any stored secret as potentially compromised until verified.

What to do now

1. Inventory all Azure API Management instances, including Classic, Developer, Basic, Standard and Premium tiers.
2. Apply Microsoft's published guidance to identify and replace potentially exposed credentials, tokens and passwords.
3. Move secrets stored directly in APIM to Azure Key Vault and align with Microsoft's security recommendations.
4. Review APIM and related identity logs for unusual token use or access since mid-November.
5. Add this event to your incident response and third-party risk processes, and brief OT and energy teams where applicable.