Microsoft fixes Azure API Management flaw as actor hunts for customer secrets



Norway's NSM says a flaw in Microsoft Azure API Management affected several Norwegian businesses, including Equinor and Skagerak Energi. An unknown actor searched for access tokens, secrets and named values. Microsoft has fixed the flaw.

- Norway's National Security Authority (NSM) disclosed a vulnerability in Microsoft Azure API Management (APIM).
- Multiple Norwegian businesses were affected, including the energy companies Equinor and Skagerak Energi.
- An unknown actor was actively looking for access tokens, secrets and named values in APIM.
- Microsoft has fixed the flaw, according to the report headline.
- The source excerpt does not give technical details or the full extent of the impact.

Norway's National Security Authority (NSM) has disclosed that it learned of a vulnerability in Microsoft's Azure API Management (APIM) that affected multiple businesses in the country. Among them are the energy companies Equinor and Skagerak Energi.

What is known

According to NSM, an unknown actor was actively searching APIM for access tokens, secrets and named values. These are the kinds of items that can open the door to connected systems and data. The report's headline states that Microsoft has fixed the flaw affecting the classic tier of the service.

The excerpt available to us does not explain how the flaw works, how many organisations were affected, or whether any data was misused. We have therefore not drawn conclusions on those points.

Why it matters for Saudi institutions

Any organisation that uses APIM to publish or protect APIs may hold credentials and configuration values inside the service. If a platform-side flaw exposes them, the risk extends to every system those values unlock. Energy and other critical-sector operators in the Kingdom should treat this as a prompt to review how secrets are stored and rotated in their API gateways.

A calm, methodical review is appropriate: confirm exposure, check for unusual activity, and rotate sensitive values where there is any doubt. Follow Microsoft's and NSM's guidance as further detail is published.

What to do now

1. Inventory all Azure API Management instances, including classic-tier ones, and confirm the fixes from Microsoft are applied.
2. List the access tokens, secrets and named values stored in APIM and rotate any whose exposure cannot be ruled out.
3. Move sensitive values to a dedicated secrets vault with restricted access where feasible.
4. Review APIM and Azure activity logs for unusual reads of secrets or configuration values.
5. Include API gateway platforms in third-party and cloud risk reviews aligned with NCA ECC and NCA CCC requirements.