Azure API Management flaw exposed secrets; Norwegian energy firms affected



Microsoft is notifying customers of a flaw in Azure API Management Classic that may have exposed stored secrets. Norway's NSM links it to incidents at Equinor and Skagerak Energi and urges affected users to treat secrets as compromised.

- Microsoft found the issue in Azure API Management (APIM) on November 18 and closed the access path the next day.
- Exposed data can include named values, identity-provider client secrets, subscription keys and tokens for APIM management APIs.
- APIM Classic tiers that do not follow Microsoft's documented security guidance are affected; v2 tiers are not.
- Norway's NSM says several organizations were hit, including Equinor and Skagerak Energi, and that

other sectors in Norway and abroad are impacted.

- The scale of exploitation is unclear.

What happened

Microsoft is informing customers of a security issue in Azure API Management (APIM), the service used to publish, secure and manage APIs. According to a customer notification shared publicly, Microsoft identified the problem on November 18 and closed the access path the following day. Microsoft states that an unauthorized party could have used the flaw to reach secrets stored in APIM Classic instances before it was found.

Norway's National Security Authority (NSM) said on November 20 that the vulnerability affected several organizations in the country, among them the energy companies Equinor and Skagerak Energi, which had separately disclosed incidents the week before. Equinor reported no evidence of stolen or altered data. Skagerak Energi said operations and production were not affected and it found no evidence of information compromise.

Who is exposed

The issue concerns APIM Classic tiers that do not follow Microsoft's documented security guidance. Instances on v2 tiers are not affected. Data at risk includes named values, client secrets for identity providers, subscription keys and tokens for APIM's direct management APIs. NSM says an unknown actor targeted tokens, secrets and named values, and that several sectors in Norway and abroad are affected. How widely the weakness was exploited remains unclear.

A security expert, Anders Kristiansen, cautioned that credentials taken from APIM could be used against external services, with the damage depending on each credential's permissions.

What NSM advises

APIM users should treat their secrets and named values as compromised and replace them, confirm their instances have been updated, and work out which data is reachable through the service.

What to do now

1. Inventory Azure APIM instances and identify any on Classic tiers, including those run by vendors on your behalf.
2. Treat all named values, identity-provider client secrets, subscription keys and management API tokens in Classic instances as compromised and rotate them.
3. Confirm with Microsoft's notification and your tenant that instances are updated and follow Microsoft's documented security guidance.

4. Map which backend systems and external services each APIM credential can reach, and review their logs for unusual access.
5. Where APIM supports critical or OT-adjacent services, report suspected exposure through your incident process and, as applicable, to NCA and your sector regulator.