NSM shares vulnerability mitigation measures in Azure API Management

Published: 20.11.2026 Updated: 23.11.2026

Earlier this week, NSM became aware of a vulnerability in Azure API Management (APIM) that affects several Norwegian businesses. Now the vulnerability is said to be closed. Nevertheless, NSM urges organizations to take measures.

- Since the vulnerability became known, NSM has worked purposefully to understand its significance as well as to map its scope and possibly other affected organizations. It is still uncertain how extensive the exploitation of the vulnerability is, and has been. So far, NSM has no evidence that compromise or attempts at compromise have had consequences for deliveries at Norwegian companies, says Martin Albert-Hoff, Director of Operational Cybersecurity at NSM.

Measures

Vulnerability: An unknown actor has actively targeted access tokens, secrets, and named values in APIM.

- Everyone who has Azure API Manager must assume that their secrets and named values are compromised. This means the business must rotate all tokens and secrets.
- It is also important that organizations map out the information behind their APIM instance to uncover the potential scope if evidence of compromise is found.
- Businesses should check whether their APIM instance has been updated. **Follow the user manual:**

Open https://<your-gateway-hostname>/internal-status-0123456789abcdef and read RuntimeVersion

- 0.52.x: patched if the last number (x) is 31936 or higher
- 0.53.x: patched if the last number (x) is 31938 or higher
- Other patterns (for example 0.53.4608.0 or 0.52.4150.0): V2 or Consumption tier where this threshold does not apply is not vulnerable
- Lower numbers, still vulnerable

If the entity's entity has not been updated, NSM asks the entity to contact the supplier directly. **If the company sees signs of, or has confirmed, compromise, we ask the company to contact NSM.**

High risk level

Equinor and Skagerak Energi are among the companies that have been affected. The vulnerability was first discovered by the Norwegian energy sector, which works well with preventive security.

- NSM wishes to commend Equinor for good work that led to early detection as well as rapid sharing with NSM and the sectoral response teams, says Albert-Hoff.

The vulnerability affects several sectors in Norway and also beyond Norway's borders. NSM maintains close dialogue and cooperation with national and international partners and organizations regarding the situation.

When a vulnerability becomes known, more actors may try to exploit it. Rapid escalation in the use of artificial intelligence (AI) is affecting the situation. This poses a risk for Norwegian businesses.

- Det nasjonale cyberrisikonivået er høyt. Siste ukers hendelser bekrefter at risikoen for cyberoperasjoner er høy. Det er derfor viktig at virksomhetene som benytter tjenesten Azure API Management iverksetter tiltakene som NSM deler, sier Martin Albert-Hoff.

- Les også: NSM hever det nasjonale cyberrisikonivået til HØYT

Et høyt risikonivå krever at norske virksomheter iverksetter forebyggende tiltak umiddelbart. Det er også årsaken til at NSM har gått offentlig ut med cyberrisikonivået for noen uker siden. Det er helt nødvendig å styrke både motstandsdyktigheten og evnen til å håndtere cyberoperasjoner i norske virksomheter. NSM har delt mange tiltak, som vi ønsker at virksomheter iverksetter. Alle tiltakene ligger på nsm.no.

Artikkelen er oppdatert 23. november. Det stod ved en feiltakelse at “sårbarheten ble først oppdaget av den norske kraftsektoren”. Dette er rettet til energisektoren.

Finner du det du leter etter?

JA

NEI