Azure API Management Classic flaw exploited to steal stored API credentials



Microsoft has warned that a flaw in Azure API Management (APIM) Classic tiers was exploited to steal stored API credentials. Norwegian authorities link it to attacks on energy companies.

- Microsoft is warning customers about a vulnerability in Azure API Management (APIM) Classic tiers.
- The flaw was exploited to steal API credentials stored in the service.
- Norwegian authorities linked the flaw to cyberattacks against energy companies.
- The source excerpt does not provide a CVE number, patch details or the number of affected customers.

Microsoft has told customers that a security vulnerability in the Classic tiers of Azure API Management (APIM) was exploited in real attacks to steal API credentials stored in the service. Norwegian authorities have tied the

flaw to cyberattacks against energy companies.

What is known

The available excerpt of the report is brief. It confirms the affected component (APIM Classic tiers), the impact (theft of stored API credentials) and the link made by Norwegian authorities to attacks on the energy sector. It does not give a CVE identifier, a technical description, the exploitation period or the number of organisations affected, so none of these should be assumed.

Why it matters

API credentials often grant access to backend systems, partner integrations and data services. If they were exposed, an attacker may be able to use them without triggering the usual login controls. Institutions running APIM Classic tiers should therefore treat this as a potential credential-exposure event rather than only a patching task.

The energy-sector targeting is relevant to Saudi operators of critical infrastructure and to financial institutions that depend on the same cloud service.

Recommended approach

Confirm whether your organisation uses APIM Classic tiers, follow Microsoft's customer guidance, and review any credentials held in the service. Full details should be taken from Microsoft's own notice, as the source excerpt is limited.

What to do now

1. Identify any Azure API Management instances on Classic tiers across your subscriptions.
2. Review Microsoft's customer notice and apply its remediation guidance.
3. Rotate API keys, secrets and other credentials stored in or managed through affected APIM instances.
4. Review API and backend access logs for unexpected use of those credentials.
5. Brief the CISO and, where relevant, notify your regulator or sector authority in line with incident-reporting obligations.