Azure APIM credential theft incident

INCIDENT · CYBER DESK

Compiled by machine from news coverage; not reviewed analysis. A snapshot taken on 23 Nov 2026. Numbers in brackets point to the Sources list at the end. The live page: https://morningstarsecurity.com/wiki/azure-apim-credential-theft-incident

FACTS

- **Date:** 2026-11-18 (low confidence, 1 independent source) [1]
- **Impact:** Unauthorized access to secrets, named values, client secrets, subscription keys, and tokens stored in APIM instances (low confidence, 1 independent source) [1]

ENTRY

Azure APIM credential theft incident is an incident mentioned in the news MorningStar covers.

Drawn from 1 news source; the facts and relationships below show where each detail comes from.

CONNECTIONS

Links to other wiki entries, from the wiki's graph. This file gives no source for them: treat them as leads, not findings.

- **Targets:** Energy Sector, Equinor

ABOUT MORNINGSTAR SECURITY

MorningStar Security is a security news reader and community, started in 2009 and relaunched in 2026. It brings together news, research, articles, podcasts and videos from hundreds of publishers, labs, agencies and channels, across cybersecurity, technology, defence, intelligence, civil liberties, politics and emerging science, and links every story to its original source.

Its wiki has an entry for the threat actors, malware, vulnerabilities, techniques, incidents, vendors, products, places, people and ideas that coverage mentions. Each entry is compiled by machine from the stories the site indexes. Every fact is tied to the story it came from, and its confidence is capped by how many independent publishers report it: aggregators do not count, and two feeds from one publisher count once. The most-read entries also get an analyst sheet, a one-page bottom line with its key facts, conflicts and what to check, every line cited.

Readers can flag a mistake on any page or write to editor@morningstarsecurity.com.

- This entry, live: https://morningstarsecurity.com/wiki/azure-apim-credential-theft-incident

- More incidents: https://morningstarsecurity.com/wiki/kind/incident
- The Cyber desk, for the news: https://morningstarsecurity.com/desk/cyber
- The whole wiki: https://morningstarsecurity.com/wiki
- About MorningStar Security: https://morningstarsecurity.com/about
- How the site is made: https://morningstarsecurity.com/editorial
- The newsletter: https://morningstarsecurity.com/newsletter

SOURCES

1. Norway links energy firm cyberattacks to critical Azure API Management flaw · The Register: Security · 23 Nov 2026 · https://www.theregister.com/security/2026/11/23/norway-links-energy-firm-cyberattacks-to-critical-azure-api-management-flaw/5311598

Snapshot of https://morningstarsecurity.com/wiki/azure-apim-credential-theft-incident taken 23 Nov 2026 18:13 UTC. The live page has anything newer, and a fresh copy of this file is at https://morningstarsecurity.com/md/wiki/azure-apim-credential-theft-incident