مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Azure API Connection Flaw Enables Cross-Tenant Compromise

Tracking #:432317634
Date:25-08-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Microsoft Azure's API Connection (APIM) infrastructure, which could allow attackers to achieve cross-tenant compromise of sensitive cloud resources.

## TECHNICAL DETAILS:

A critical security vulnerability has been discovered in Microsoft Azure's API Connection architecture, allowing attackers to gain administrative access across multiple tenant environments. Exploitation could expose sensitive data stored in Azure Key Vaults, Azure SQL databases, and third-party services integrated via API Connections, including Jira, Salesforce, and Slack.

**Vulnerability Details:**

- Vulnerability Type: Multi-tenant privilege escalation due to shared APIM architecture.
- Attack Vector: Abuse of undocumented DynamicInvoke API endpoint.
- Key Issue: Requests executed with global ARM tokens instead of tenant-scoped tokens.
- Exploit Mechanics:
  - Attacker with Contributor role to any API Connection can craft malicious requests.
  - DynamicInvoke allows arbitrary requests with custom paths, headers, and body.
  - Path traversal payloads (../../../../[VictimConnectionID]) normalize into another tenant's space.
  - Result: Full access to victim API Connection resources.

**Impact:**

Successful exploitation grants:

- **Azure Key Vaults:** Full access to secrets, certificates, and cryptographic keys
- **Azure SQL Databases:** Complete database access, potential data exfiltration
- **Third-party integrations:** Compromise of services such as Slack, Salesforce, Jira
- **Externally connected resources:** Full administrative privileges

**Requirements for Exploitation:**

Contributor-level access to any API Connection in any Azure tenant.

**Mitigation:**

- Blacklisting path traversal sequences such as ../ and certain URL-encoded variants in path parameters.
- Further bypasses may still be possible through alternative path normalization techniques. Defense-in-depth hardening is recommended.

**Affected Component:**

- Microsoft Azure API Connections
- Shared Azure API Management (APIM) instance used globally

## RECOMMENDATIONS:

- Restrict API Connection permissions to the minimum required.
- Avoid using Contributor accounts for sensitive API Connection operations where possible.

- Review and rotate secrets in Azure Key Vaults connected via API Connections.
- Monitor for unusual API Connection activities and Logic App manipulations.
- Continue security testing for path traversal and DynamicInvoke misuse.
- Conduct additional penetration testing for cross-tenant access risks.
- Apply security updates and follow Microsoft's mitigation guidance.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- https://binarysecurity.no/posts/2025/08/azures-weakest-link-part2