مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Azure Default API Connection Flaw Enabling Cross-Tenant Compromise

Tracking #:432317630

Date:24-08-2025

TLP: WHITE

Executive Summary

A critical vulnerability[i] in Microsoft Azure's API Connection framework, disclosed on April 7, 2025, allows attackers with Contributor-level access to any API Connection to achieve full cross-tenant compromise. This flaw, rooted in the shared API Management (APIM) instance and an undocumented DynamicInvoke endpoint, enables unauthorized access to sensitive assets like Azure Key Vaults, SQL databases, and third-party integrations (e.g., Jira, Salesforce). Microsoft provided mitigations, blacklisting path traversal patterns, but concerns about potential bypasses persist. This advisory details the exploit's mechanics and provides actionable recommendations to secure Azure environments.

Technical Analysis

Vulnerability Overview:

Component Affected: Azure API Connections via shared APIM instance.

Impact: Full cross-tenant compromise, granting administrator-level access to API Connections and associated resources.

Access Level Required: Contributor-level access to any API Connection in any tenant.

Endpoint Exploitation: Undocumented DynamicInvoke endpoint in Azure Resource Manager (ARM).

Attack Vector:

- Unlike the restricted /extensions/proxy/[Action] endpoint, DynamicInvoke permits arbitrary HTTP methods, paths, headers, and bodies.
- ARM constructs requests using /apim/[ConnectorType]/[ConnectionId]/[Action-Endpoint] with super-privileged tokens.
- Attackers craft custom Logic App connectors with path traversal payloads (e.g., ../../../../[VictimConnectorType]/[VictimConnectionID]/[action]), bypassing access controls and targeting victim connections.

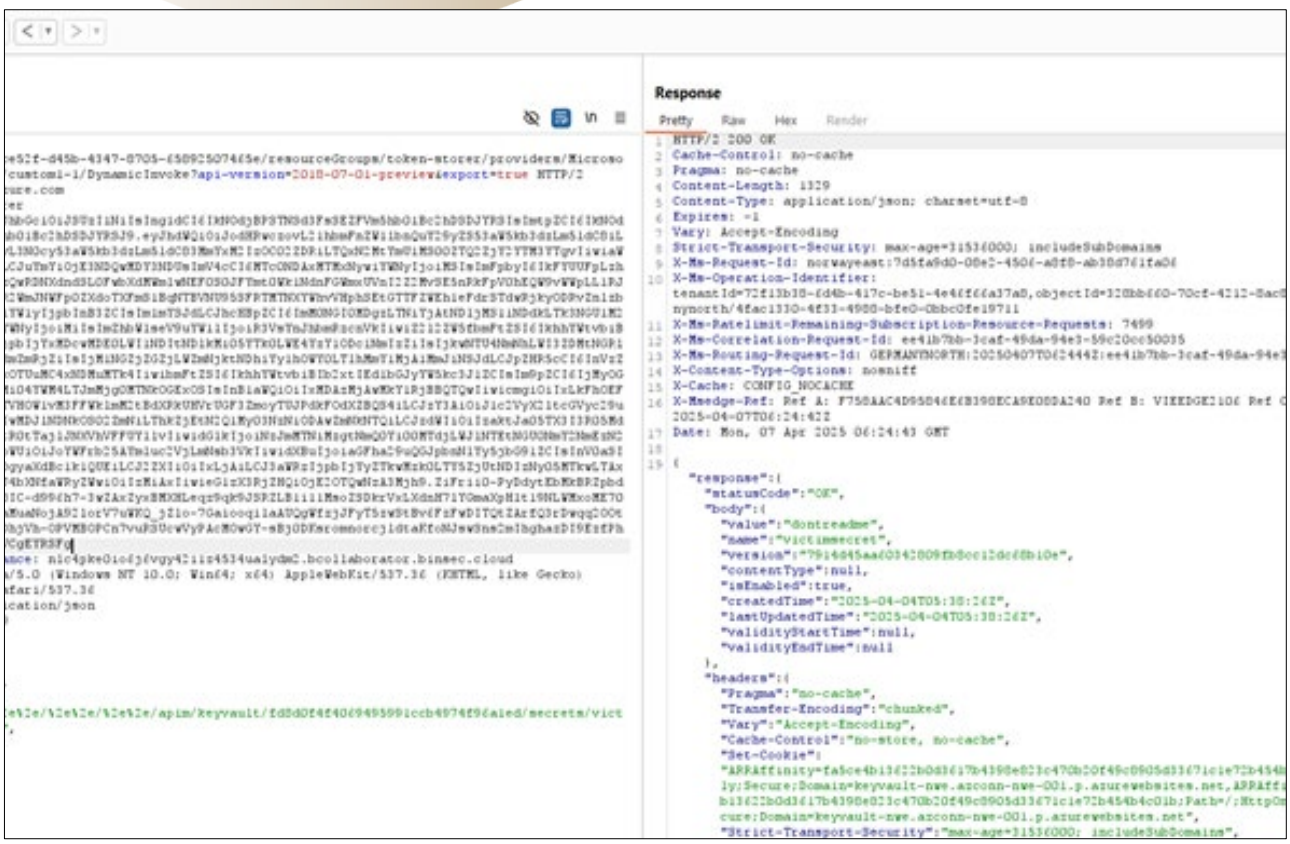

Figure 1: Traverse to a victim connection and retrieve Secrets

Assets at Risk:

- Azure Key Vaults: Access to secrets, certificates, and keys.
- Azure SQL Databases: Potential data exfiltration or manipulation.
- Third-Party Services: Compromised integrations with Slack, Salesforce, Jira, etc.

Mitigation Strategy: Blacklisting of ../ and URL-encoded variants in path parameters. Limitations: Potential bypasses via alternative path normalization or direct endpoint manipulation remain under investigation.

Recommended Actions

For Security Teams:

- Audit API Connections: Review Logic Apps and API Connections for custom connectors or suspicious configurations.
- Check for DynamicInvoke usage or unusual path parameters.
- Restrict Contributor Access: Limit Contributor roles to trusted personnel only.

- Use Just-In-Time (JIT) access and Privileged Identity Management (PIM) to minimize exposure.
- Monitor for Exploitation: Enable detailed logging for API Management and Logic App activities.
- Set alerts for path traversal attempts or unauthorized API Connection access.

For Cloud Architects

- Strengthen Multi-Tenant Isolation: Avoid reliance on shared APIM instances for sensitive workloads.
- Explore tenant-specific APIM instances where possible.
- Implement Defense-in-Depth: Apply network segmentation and firewall rules to isolate critical resources.
- Enforce additional authentication for high-value services like Key Vaults.

For Microsoft Azure Customers:

- Engage Microsoft Support: Confirm your tenant's status and inquire about additional patches or updates.
- Stay updated on Microsoft's ongoing investigation into potential bypasses.
- Conduct Penetration Testing: Perform red team exercises targeting Logic Apps and API Connections.
- Validate the effectiveness of Microsoft's mitigations in your environment.

References

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