Mphasis
The Next Applied

Azure Service Tags Vulnerability: Microsoft Warns of Potential Abuse by Hackers

Date: 11th June 2024 | Severity: High

Summary

Microsoft is warning about the potential abuse of Azure Service Tags by malicious actors to forge requests from a trusted service and get around firewall rules, thereby allowing them to gain unauthorized access to cloud resources.

Attack Vectors

- Tenable Research has discovered a vulnerability in Azure that allows an attacker to bypass firewall rules based on Azure Service Tags by forging requests from trusted services. Customers who rely on these firewall rules for security are at risk from this vulnerability. They should take immediate action to mitigate the issue and ensure they are protected by robust layers of authentication and authorization.
- The vulnerability was discovered initially in the Azure Application Insights service, but we and the Microsoft Security Response Center (MSRC) eventually found that it affects more than 10 other Azure services those include.
  - Azure Application Insights
  - Azure DevOps
  - Azure Machine Learning
  - Azure Logic Apps
  - Azure Container Registry
  - Azure Load Testing
  - Azure API Management
  - Azure Data Factory
  - Azure Action Group
  - Azure AI Video Indexer

Indicator of compromise

INDICATOR TYPE	INDICATORS
Vulnerability	• Multiple services in Azure allow the customer to craft web requests. Some even allow users to add headers to the request and to change HTTP methods. This is part of the intended functionality of these services. For example, since the Azure Application Insight Availability Tests Feature tests the availability of applications deployed by clients, clients require full control of the request to create a functional test. • However, this functionality may open the door for a malicious actor to achieve an impact similar to that of a server-side request forgery (SSRF) vulnerability. SSRF allows an attacker to cause a server-side application to make requests to an unintended location, whether internal or external, allowing the attacker, among other options, to reach/expose resources that were previously unreachable.
Impact	• This vulnerability enables an attacker to control server-side requests, thus impersonating trusted Azure services. This enables the attacker to bypass network controls based on Service Tags, which are often used to prevent public access to Azure customers' internal assets, data, and services.

Recommendation

- Service Tags are not sufficient to secure traffic to a customer's origin without considering the nature of the service and the traffic it may send. It is always the best practice to implement authentication/authorization for traffic rather than relying on firewall rules alone.
- Microsoft strongly recommends that customers proactively review their use of service tags and validate their security measures to authenticate only trusted network traffic for service tags.

Reference Links

- https://www.tenable.com/blog/these-services-shall-not-pass-abusing-service-tags-to-bypass-azure-firewall-rules-customer
- https://thehackernews.com/2024/06/azure-service-tags-vulnerability.html