BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

June 17, 2024

Microsoft Alert for Hacker Exploitation of Azure Service Tags Vulnerability

Summary

Microsoft warns of Azure Service Tag exploit by malicious actors to bypass firewall rules and gain unauthorized access to cloud resources, highlighting the inherent risk of relying solely on service tags for network security.

Technical Details

Azure Service Tags simplify network isolation within Azure by grouping specific Azure services IP ranges. These tags can be used to define network security rules and apply these rules consistently across multiple Azure resources. Essentially, Azure Service Tags provide a convenient way to manage access controls, such as firewall rules or network security group (NSG) configurations.

Microsoft issued a warning about the potential misuse of Azure Service Tags, which could allow attackers to forge requests from a trusted service and bypass firewall rules. This issue, highlighted by Tenable, reveals that Azure customers who depend on service tags for firewall rules could be vulnerable. At least 10 Azure services are affected: 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, and Azure Chaos Studio.

The core problem arises when an attacker in one tenant can send crafted web requests to access resources in another tenant if the latter has allowed traffic from the service tag without additional authentication. This vulnerability allows the attacker to manipulate server-side requests and impersonate legitimate Azure services. Consequently, the attacker can circumvent network controls that rely on Service Tags, which are typically used to block public access to Azure customers' internal assets, data, and services.

Recommendations

- Analyze the network rules for each associated service in your Azure environment, identify the use of Service Tags, and filter out the affected services. Assume that assets using these Service Tags are public.
- Add authentication and authorization layers to the affected services. Follow the MSRC guidance: "Service Tags alone are not sufficient to secure traffic to a customer's origin. Implement authentication/authorization for traffic rather than relying solely on firewall rules."
- When configuring network rules, remember that Service Tags do not provide airtight security. Ensure strong network authentication is maintained to provide an additional layer of security. This extra layer can significantly hinder an attacker, even if they manage to leverage the vulnerability to reach the target endpoint.
- Pay particular attention to the Azure services listed as vulnerable. Approach other services not listed with skepticism and check for the dangerous combination described. Conduct regular security audits to ensure that your network rules and security measures are up to date. Monitor for any changes in service behavior or new vulnerabilities.
- Stay abreast of the latest security recommendations from Microsoft and other cybersecurity authorities. Apply patches and updates as soon as they are available to mitigate known vulnerabilities.

References

- https://thehackernews.com/2024/06/azure-service-tags-vulnerability.html

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