Microsoft Says Azure Cloud Attack Scenario Isn't a Flaw

Redmond Calls Tenable Report Evidence of Customers Misconstruing Azure Service Tags

BY David Perera (@daveperera) • June 6, 2024 (link)

Microsoft is calling security research asserting a high-severity vulnerability exists in Azure evidence that customers should better configure their cloud environments.

Security firm Tenable on Monday published a blog post that details how attackers could bypass firewall rules based on Azure Service Tags. Service Tags group IP addresses used by Azure services, the better to allow firewall whitelisting for functions such as an availability test.

An attacker with an Azure instance - legitimately obtained or not - could obtain access to company resources by sending customizable HTTP requests to web applications through an Azure service that firewalls are configured to let through. The flaw exists in more than 10 Azure services including API management, Tenable found.

"The core of the issue is that it doesn't matter if it's me using my available test service or somebody setting up an availability test service - the traffic would still go through," said Noam Dahan, a Tenable research manager.

Microsoft said Monday it has not seen any such attacks in the wild or received reports of them.

Tenable and Microsoft each say that the computing giant responded to Tenable's disclosure of the attack proof of concept in January by awarding a bug bounty to the cybersecurity company.

But as it examined the issue in later months, Microsoft decided that Tenable had not in fact uncovered a server-side request forgery flaw or a firewall bypass vulnerability. Azure customers apparently are misunderstanding "how to use service tags and their intended purpose," the company wrote Monday.

"Service tags are not a comprehensive way to secure traffic to a customer's origin and do not replace input validation to prevent vulnerabilities that may be associated with web requests."

Rather, Tenable's findings highlight the need for authenticating web requests, the company concluded. "We encourage customers take a multi-layered security approach when it comes to validating their security measures to authenticate only trusted network traffic for service tags," a company spokesperson said in an emailed prepared statement.

Dahan told Information Security Media Group that Tenable still believes it uncovered a security vulnerability. Authentication will add another layer of security, he said, but it doesn't cure the underlying problem. "Authentication is a complete security discipline, where you can get some things right and get some things wrong. That is not something that customers will get right 100% of the time," he said.

There are potential limitations for attackers, Dahan said. Hackers would need to know or guess the target Azure domain. "In some cases, the URL being unknowable would make the attacker's life difficult, but that is not a security standard by itself," he said. That information could leak out - code repositories are notorious for exposing internal data that shouldn't be public - or hackers might simply deduce the domain.

Microsoft's advice to companies is to add authentication tokens to HTTPS headers.