Tagging Falsely (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

AWS and Azure allow cloud users to tag resources with arbitrary labels ostensibly for accounting and management purposes. It is often a good practice to use this tagging information in detection engines and in making automated security decisions. If an adversary is able to discern the tagging protocol, he can alter tags for newly created services to potentially avoid detection or to circumvent security mitigations.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **Mitigation** | **Description** |
| Limit Rights to Add or Modify Tags | Azure does not currently allow you to limit tagging of a resource you already have contributor or owner rights to. However changes to the tags will be reflected in API logs in both AWS and Azure. |

Detection

Tag results are recorded in Cloud API logs. Multiple concurrent tag changes that are not part of some CI/CD process are likely rare and should be viewed with suspicion

References

1. https://social.msdn.microsoft.com/Forums/azure/en-US/580ce000-e413-455d-a4b2-9a512e6da018/restrict-tag-value-modification?forum=WAVirtualMachinesforWindows. Accessed June 12, 2020