Exploit S3 (Simple Storage Service) Permissions (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Adversaries may be able to exploit the permissions of S3 buckets to be able to gain access and exfiltrate data. S3 buckets are Amazon’s Simple Storage Services. They are used to store data such as log files, JavaScript libraries, system backups, images, etc.. This service allows users to store and access data easily, but can be an issue if permissions are not configured properly. This can lead to read access, download permissions to anyone who views the bucket, and open upload permissions, both of which can be exploited by an adversary.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Rhino Security Labs Blog Post | In this walkthrough the adversary first finds the region in which they wish to exploit. Once the region is determined they then start to probe for buckets. This is accomplished by general querying and enumeration of bucket names. To determine if a bucket is found that has unfettered access permissions the command, “sudo aws s3 ls s3://$bucketname/ --region $region” can be run with the expectation of returning a directory listing. Once the S3 bucket is identified if an open upload policy can allow an adversary to upload malicious Javascript (or other scripts that are able to perform malicious activity) to all application users. Depending on permissions set buckets can allow for system backups to be downloaded, as well as source code, log files that may contain usernames and passwords, and other critical information. This was tested utilizing Alexa’s top 10,000 sites which resulted in 107 buckets. 57% of the buckets had download permissions to anyone who viewed them, 12% had open upload permissions, and 8% had both permission errors. |
| Twilio S3 Bucket Exploited | The attackers found an open S3 bucket to exploit. Once this was found the JavaScript SDK was altered. The development kit was vandalized as part of an automated cyber-crime campaign that preys on JavaScript code in open S3 buckets to inject malicious ads into browsers. |

Mitigations

|  |  |  |  |
| --- | --- | --- | --- |
| **Mitigation** | | **Description** | |
| Web Application Firewall | | Ensuring that cloud applications are configured behind a web application firewall can make it harder for an adversary to determine a target’s IP address. | |
| Least Privilege |  | | All access given to users in the cloud environment should be assigned by the necessary privileges needed for team members to complete their job responsibilities. Ensure that temporary access tokens are issued rather than permanent credentials, especially when access is being granted to entities outside of the internal security boundary . |
|  | AWS | | To implement least privilege in an AWS environment IAM policies will be used. This gives the ability to allow users to perform list, read, write, permissions management, or tagging actions. AWS suggests utilizing *last accessed information* and A*WS CloudTrail event history* to get a better understanding of privileges that might be needed or reduced based on a specific role. Full details can be found at [**https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege**](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege)**.** |
|  | Azure | | To implement least privilege in an Azure environment Azure Active Directory roles will be used. Azure outlines different tasks and the least privileged role that are suggested to be associated with the task. Those details can be found at:[**https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-delegate-by-task**](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-delegate-by-task)**.** To learn how to assign specific roles it can be done via the Azure Active Directory Portal. Instructions on how to assign roles can be found here: [**https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-manage-roles-portal**](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-manage-roles-portal)**.** |
|  | GCP | | [To implement least privilege in GCP it](https://cloud.google.com/blog/products/application-development/least-privilege-for-cloud-functions-using-cloud-iam) is recommended to use predefined roles (which allow for granular access permissions) instead of primitive roles (roles/owner, roles/editor, and roles/viewer). Full details on the difference between types of roles can be found here: [**https://cloud.google.com/iam/docs/understanding-roles**](https://cloud.google.com/iam/docs/understanding-roles)**.** To assign these roles IAM service accounts are used and complete details can be found at: [**https://cloud.google.com/iam/docs/using-iam-securely#least\_privilege**](https://cloud.google.com/iam/docs/using-iam-securely#least_privilege)**.** |

Detection

This can be detected by unknown uploads or downloads to/from the S3 buckets.

References

1. https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-storage/. Accessed June 30, 2020.