Abusing Cloud Storage for Access (including S3/Blob manipulation) (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Cloud storage repositories like Azure containers and AWS S3 buckets are really convenient places to store code for use by developers who are developing apps within the cloud. They can be also serve out content via HTTPS to allow public consumption of new code. Although often intended as a temporary solution while working on more challenging aspects of code development, storing code in cloud storage can unintentionally be incorporated into production, leaving consumers of this software vulnerable to code modification when a container or bucket is misconfigured. Adversaries can modify code stored in buckets to implant backdoor software to gain a foothold in what would otherwise be a well-protected enclave. If a storage bucket used for hosting code is ever deleted in the future, adversaries can reclaim the bucket name and without any special privileges stage code for unsuspecting people to invoke. This is especially problematic if web servers are pointing at the repo to fetch some forgotten piece of code.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Hackerone | The Rocket Chat install application was grabbing code from a publicly accessible S3 bucket. When the S3 bucket was deleted, this made the situation even worse. Once a bucket is deleted, anyone with access to AWS can create a bucket of the same name. In this case putting a malicious script within the bucket and waiting for unsuspecting users of the Rocket Chat installation script to fetch and run their payload. |
| Subjack | Open source tool that automates the search for s3 buckets and other cloud resources that are registered in DNS but which no longer exist indicating a possible hijacking opportunity. |

Mitigations

|  |  |  |
| --- | --- | --- |
| **Mitigation** | | **Description** |
| Audit | | Frequently check permissions on cloud storage to ensure proper permissions are set to deny open or unprivileged access to resources. Consider using automated resource checkers such as CloudSploit or Divvycloud. |
|  | AWS | To perform an audit via AWS it is suggested to review information such as account details (credentials, users, groups, roles, etc), mobile applications, EC2 configurations, policies, and account activity. How to audit these different factors can be found in detail at: **https://docs.aws.amazon.com/general/latest/gr/aws-security-audit-guide.html.** |
|  | Azure | To perform an audit via Azure an administrator can review the audit logs that are recorded under Azure’s monitoring for active directory. The audit logs allow for filtering, as well as looking at users, groups, and enterprise specific information. Full details on how to access this information can be found at: **https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs.** |
|  | GCP | To perform an audit via GCP the logs can be reviewed. GCP breaks this down into three categories; admin activity, data access, and system events. The audit logs can be viewed a few different ways- the console, API, or gcloud. Full details on how to view these logs, how to export, and for how to configure the retention period can be found here: **https://cloud.google.com/logging/docs/audit.** |
| Don’t Do it | | Don’t store executable code within cloud storage repos. |
| Encrypt Sensitive Information | | Encrypt data stored at rest in cloud storage. Managed encryption keys can be rotated by most providers. At a minimum, ensure an incident response plan to storage breach includes rotating the keys and test for impact on client applications. |
|  | AWS | To encrypt data at rest in an AWS environment first start by configuring the IAM roles and permissions. A policy will need to be created to specify that the data is to be encrypted and then the policy is attached to the instance. Full details on how to accomplish this can be found at: **https://aws.amazon.com/blogs/security/how-to-protect-data-at-rest-with-amazon-ec2-instance-store-encryption/**. |
|  | Azure | To encrypt data at rest in an Azure environment it can be done differently depending on the cloud service the customer is utilizing. For SaaS customers this can be enabled or available on each specific service. For PaaS customers there are specific storage and application platforms that can be used. In terms of IaaS customers this can be broken down to a couple different aspects. Encrypted storage can be enabled the same as PaaS services, utilizing other Azure services. Encrypted compute allows for all managed disks, snapshots, and images to be encrypted utilizing a service managed key. The keys are stored in the Azure key vault. Full details on how to accomplish this can be found at: **https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest.** |
| 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.** |
|  | 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.** 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.** |
|  | 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.** 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.** |

Detection

Monitor for unusual queries to the cloud provider's storage service. Activity originating from unexpected sources may indicate improper permissions are set that is allowing access to data. Audit storage locations for executable files frequently.

References

1. https://hackerone.com/reports/399166. Accessed 02/12/2020
2. https://securityonline.info/subjack-hostile-subdomain-takeover-tool/ Accessed 08/12/2020