IAM Abuse (version 1.0)

**Cloud Service Label: IaaS, PaaS**

Description

Both Azure and AWS employ IAM functionality that assigns specific resource roles to either users, groups, or service principals in an attempt to limit permissions to only those required to perform required tasks. Using the credentials of any user or service principal, cloud API’s can be used to scan all available roles that may have been assigned. Because of the hundreds/thousands of roles available, administrators may not realize or remember which roles are assigned to whom. Even AWS can get confused, in 2018 AWS released a recommended managed policy that inadvertently allowed any user assigned this role the ability to grant all accesses to all AWS account resources.

Adversaries can use tools such as Pacu to discover obscure role assignments and use these accesses to further infiltrate the cloud infrastructure.

Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| iam\_\_privesc\_scan | Abuses AWS API to list all roles an account has been granted and suggests further actions based on these roles. |
| Validate\_iam\_principals.py | Open source Module that scans for available IAM roles in a given account. |
| AmazonElasticTranscoderFullAccess | Abuses flaw in AWS IAM managed policy to enable assignment of arbitrary permissions to any other IAM role. |
| aws\_escalate.py | AWS\_escalate.py is a script written by Rhino Security Labs that detects over 20 possible privilege escalation methods within an AWS environment when provided with an access key and secret key. For example, *python3 aws\_escalate.py –all-users –access-key-id ABCDEFGHIJK –secret-key hdj6kshakl31/1asdhui1hka* will check privilege escalation methods for all users. |
| PowerZure | PowerZure is a GitHub project that automates the process of assessing and exploiting resources and misconfigurations within Azure. |

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. Frequently check role assignments to ensure proper permissions are set and still required. Consider using automated role checkers. |
|  | 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.** |
| Azure Access Review | | Consider using account audit functionality periodically to ensure rights are still required by various accounts. |
| Setting IAM Policies and Permissions | | Implement least privilege and assign roles and permissions to users as necessary. |
|  | AWS | Amazon’s article for IAM security best practices in AWS covers topics including creating individual IAM users, using AWS managed policies, roles, frequent key rotation and others. Full details can be found at **https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html.** |
|  | Azure | Microsoft’s article for IAM security best practices in Azure covers topics including centralizing identity management, turning on conditional access, use role-based access control, using Azure AD for storage authentication, and others. Full details can be found at [**https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices**](https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices)**.** |

Detection

|  |  |
| --- | --- |
| **Detection** | **Description** |
| Create Log Metric Filters and Alarms for AWS | To create a metric filter and alarm:   1. Create a metric filter that checks for IAM policy changes and the *<cloudtrail\_log\_group\_name>* 2. Create an SNS topic 3. Create an SNS subscription to the above topic 4. Create an alarm associated with the filter and SNS topic created in steps 1 and 2 respectively |
| Monitor Activity in AWS Account | Various services in AWS offer logging features that allow for detection capabilities. These include CloudFront, CloudTrail, CloudWatch, Config, and S3. |
| Monitor for Suspicious Activity in Azure | Azure AD can generate anomaly reports than can be run on a daily basis. Azure AD Identity Protection show current risks in its dashboard and provides daily email summary notifications. Policies can also be configured to alert to specific issues. |

References

1. <https://github.com/RhinoSecurityLabs/pacu/wiki/Module-Details>. Accessed Feb 12, 2020.
2. Sharath AV AWS Security Flaw which can grant admin access! https://medium.com/ymedialabs-innovation/an-aws-managed-policy-that-allowedgranting-root-admin-access-to-any-role-51b409ea7ff0. Accessed February 13, 2020.
3. https://github.com/dagrz/aws\_pwn/tree/master/reconnaissance. Accessed Feb 20, 2020.
4. <https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/>. Accessed July 21, 2020.
5. <https://posts.specterops.io/attacking-azure-azure-ad-and-introducing-powerzure-ca70b330511a>. Accessed July 21, 2020.
6. <https://github.com/hausec/PowerZure>. Accessed July 21, 2020.
7. <https://blog.netspi.com/attacking-azure-cloud-shell/>. Accessed July 30, 2020.
8. <https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>. Accessed August 3, 2020.
9. <https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices>. Accessed August 3, 2020.