Violation Notice and Compliance Instructions

Violation:

AWS IAM/resource policies insecurely configured

Description:

Policies in your account are insecurely configured. It's dangerous to grant permissions with a wildcard (*) in the Account, Principal, or Service references or in the action reference of certain policies. Doing so can publicly expose data and make your account and resources vulnerable to cyber-attacks.

Using the wildcard as a principle reference opens it to anyone, including the public. Using the wildcard paired with AWS in the Principal reference (AWS:*) lets anyone with AWS access get access to your account.

This is not an acceptable practice. Whenever possible, use AWS Identity and Access Management (IAM) policies that identify specific resources.

If public access has been granted to any of your resources or polices, **DO NOT DELETE OR REMOVE** any items. Limit access as directed in each instruction. If the data has been accessed by unauthorized parties, these items may be required in a future forensic investigation.

AWS IAM:

Instructions for changing IAM permissions:

1. Log in to the AWS Management Console and click the **Services** tab.
2. In the **Security, Identity & Compliance** category, select **IAM**.
3. In the left navigation pane, choose **Policies**.
4. From the **Filter policies** drop-down, select **Customer managed** to review policies of that type only.
5. Click on the **Policy name** (link) of the IAM policy that you want to examine.
6. Select **Permissions** tab and click the **{} JSON** tab below it to access the selected policy document in JSON format.
7. Inside the Policy document box,

- search for statements with the following combination of elements: “**Effect**”: “Allow”, “**Action**”: “*” , ”**Resource** : “*”(all actions can be performed by the AWS resource(s) defined within the policy).

- Identify the **Action** element and If the element value is set to **"x:*" (service:*)** and **resource** is *****(all service actions can be performed by the AWS resource(s) defined within the policy statement). Update the selected policy by replacing the Action element value (i.e. "iam:*" – full IAM access) with specific service actions, based on the access plan that you want to achieve for the selected role or Restrict all actions to a specific resource.

8. Any managed policies with those elements allow full administrative privileges, which goes against security best practices. Deactivate them by detaching them from any IAM users, group or roles.
9. Repeat as needed to determine if other IAM customer managed policies provide full administrative privileges and therefore should be deactivated.

Resource policies insecurely configured

(Instructions follow for changing SNS, SQS, and ES permissions.)

Instructions for changing SNS permissions:

1. Log in to the AWS Management Console and click the **Services** tab.
2. In the **Application Integration** category, select **Simple Notification Service.**
3. In the **SNS dashboard**, select **Topics** in the left navigation pane.
4. Check the SNS topic in need of modification, then select the **Actions** dropdown.
5. Select **Edit topic policy**.
6. Select the **Only me (topic owner)** radio buttons to limit publishing messages or subscription requests to the topic owner only.
7. If you want to let others publish messages or subscribe to the topic, select the **Only these AWS users** radio buttons and enter the valid AWS account IDs of those users.
8. Click **Update policy** to apply the new permissions.

Instructions for changing SQS permissions:

Violation Notice and Compliance Instructions

1. Log in to the AWS Management Console and click the **Services** tab.
2. In the **Application Integration** category, select **Simple Queue Service**.
3. Check the box next to the queue needing modification.
4. Select the **Permissions** tab, then the **Add a Permission** button.
5. In the **Effect** section, select **Allow** or **Deny** for any specific users (identified as a **Principal**) to explicitly grant or deny permission to a specified user (principal).
6. In the **Principal** section, uncheck the **Everybody (*)** checkbox and enter the AWS account ID of the person allowed or denied permissions in the **Effect** section.
7. In the **Actions** section, click the drop-down list to select or deselect SQSpermitted requests for the principal. To grant the principal permission for all such options, check the **All SQS Actions (**SQS:***)** box adjacent to the dropdown list.

Instructions for changing ES permissions:

1. Log in to the AWS Management Console and click the **Services** tab.
2. Under the **Analytics** heading, select **Elasticsearch Service**.
3. Select the domain in need of modification.
4. On the domain's description page, click the **Modify access policy** button from the dashboard top menu.
5. On the **Modify the access policy** for **<DOMAIN NAME>** page, select one of the policy templates from the Set the domain access policy to dropdown list:
   - Select Allow or deny access to one or more AWS accounts or IAM users and provide the necessary AWS account ID/ARN or IAM user ARN to limit the ES domain access to an AWS account or IAM user only
   - Select Allow access to the domain from specific IP(s) and provide an IP address (or more IP addresses, separated by comma) to limit the ES domain access to that IP address only:
   - Select Copy an access policy from another domain and choose another ES domain name to copy its access policy:
   - Select Deny access to the domain to block entirely the access to the selected ES domain:
6. Click **Submit** to apply the access policy changes.

7. The Change your access policy dialog box, click OK to confirm the action. The ES domain status should change from Active to Processing. The status should return to Active before your modified access policy takes effect.

Instructions to restrict API gateway:

1. Sign in to the API Gateway console at https://console.aws.amazon.com/apigateway.
2. Choose the API name.
3. In the left navigation pane, choose **Resource Policy**.
4. If Effect is allow and **Principal is *** then restrict the API Gateway 5. If no resource-based policy is being used, then follow the below rules.
6. If desired, choose one of the Examples. In the example policies, placeholders are enclosed in double curly braces ("{{placeholder}}"). Replace each of the placeholders (including the curly braces) with the necessary information.
7. If you don't use one of the Examples, enter your resource policy.
8. Choose **Save**.
9. If the API has been deployed previously in the API Gateway console, you'll need to redeploy it for the resource policy to take effect.

Instructions for changing Glacier permissions:

1. Log in to the AWS Management Console and click the **Services** tab.
2. Under the **Storage** heading, select **S3 Glacier**.
3. Select a **vault name** and click on **Permissions**
4. Click on **Edit policy document**
5. Remove ***** from the **principal** element the policy and **restrict** it to specific **users** or an account. 6. Click **save**

Note: For detailed information on AWS IAM Policies. Please refer link

Getting help:

ACCENTURE CLOUD PLATFORM
Accenture Cloud Security Team

accenture

Violation Notice and Compliance Instructions

Many of these remediation instructions are simple to follow, while others are complex. We recommend you consult with your cloud application architect or infrastructure team if you are having trouble. You also may also log an incident for the attention of the Accenture Cybersecurity Command Center team using the **Self Service Portal**.

Login to Self Service Portal (SSP), choose **Support** and then select **SELF-SERVICE PORTAL**.

Please contact Cloud.Sec.Compliance if you require assistance with logging an SSP ticket.

Requesting an exemption:

In very rare instances, there are legitimate business reasons for allowing what otherwise would be deemed a security violation. If you are highly confident that you have such a reason please follow the process documented here.