Violation Notice and Compliance Instructions

Violation:

AWS NSG insecure outbound access rules

Description:

Security groups must not allow traffic to/from the internet (0.0.0.0/0) via ports that are prohibited under Accenture policy. The policy limits ports below 1024 to ports 80 and 443 only. Allowing unrestricted (0.0.0.0/0) inbound/ingress access to uncommon ports can increase opportunities for malicious activity such as hacking, data loss and all multiple types of attacks (brute-force attacks, Denial of Service (DoS) attacks, etc). For the complete rules, see https://go.accenture.com/ACPCompliancePorts

Note: An automated remediation script is available to help you bulk remediate your violations. Please see **here**

Instructions

Inbound Remediation Steps

1. Connect to console as admin user
2. In the navigation panel, under **NETWORK & SECURITY** section, choose **Security Groups**. Select the appropriate security group.
3. Select the **Inbound** tab from the dashboard bottom panel and click the **Edit** button.
4. In the **Edit inbound rules** dialog box, change the Source 0.0.0.0/0 to any restricted Cidr range for the ports which are not allowed to be open. (The inbound rules can be open to the internet 0.0.0.0/0 for only FASM approved ports)

Outbound Remediation Steps

1. Navigate to EC2 dashboard.
2. In the navigation panel, under **NETWORK & SECURITY** section, choose **Security Groups**.
3. Select the appropriate security group
4. Select the **Outbound** tab from the dashboard bottom panel and click the **Edit** button.
5. In the **Edit outbound rules** dialog box, change the traffic **Destination** for any outbound rules that allow unrestricted access (0.0.0.0/0), by performing one of the following actions:
    a. Select **My IP** from the **Destination** dropdown list to allow outbound traffic only to your machine (to your public IP address).
    b. Select **Custom** from the **Destination** dropdown list and enter one of the following options based on your access requirements:
        i. The static IP/Elastic IP address of the permitted host with the suffix set to /32, e.g. 56.160.52.238/32.
        ii. The IP address range of the permitted hosts in CIDR notation, for example

56.160.52.238/24.

iii. The name or ID of another security group available in the same AWS region.

6. Click **Save** to apply the changes.

Remediate Amazon Redshift Security Group

1. In the Amazon Redshift console, in the navigation pane, choose **Clusters.**
2. In the navigation pane, click **Security**.
3. On the **Security Groups** tab, in the cluster security group list, click the cluster security group whose rules you want to manage.
4. On the **Security Group Connections** tab, click **Add Connection Type**.
5. In the **Add Connection Type** dialog, do one of the following:

   a. Add an ingress rule based on CIDR/IP.

   - In the **Connection Type** box, click **CIDR/IP**.
   - In the **CIDR/IP to Authorize** box, specify the range. Click **Authorize**.

   b. Add an ingress rule based on an EC2 Security Group.

   - Under **Connection Type**, select **EC2 Security Group**.
   - Select the AWS account to use. By default, the account currently logged into the console is used. If you select **Another account**, you must specify the AWS account ID.
   - Click the name of the EC2 security group you want in the **EC2 Security Group Name** box.
   - Click **Authorize**.

Getting help:

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.