Violation:
Protect Private Content using CloudFront Signed URLs & Cookies for S3 Private Buckets

Description:

Your account has private content from a non-public S3 bucket that is not well protected because you are not using CloudFront Signed URLs/Cookies. If you get a violation and your distribution is using a **public S3 bucket** as an origin, please ensure that the CloudFront distribution gets Account MD approval.

Remediation Instructions:

CloudFront key pair Requirement: To create signed URLs or signed cookies, you need at least one AWS account that has an active CloudFront key pair. This account is known as a trusted signer. As soon as you add the AWS account ID for your trusted signer to your distribution, CloudFront starts to require that users use signed URLs or signed cookies to access your files so when someone requests a restricted file, CloudFront compares the signed portion of the URL or cookie with the unsigned portion to verify that the URL or cookie hasn't been tampered with. CloudFront also verifies that the URL or cookie is valid, meaning, for example, that the expiration date and time hasn't passed. **See the instructions to set up CloudFront key pair here.**

Instructions for CloudFront configuration:

1. Login to the **AWS Management Console**.
2. Navigate to **CloudFront** dashboard.
3. Select the distribution by selecting the **Check Box** for the distribution
4. Click on the **Distribution Settings** button
5. Click on the **Behaviors** tab in the Distribution Settings screen
6. Select the **Check Box** for the default path pattern and click **Edit**
7. Scroll down to **Restrict Viewer Access (Use Signed URLs or Signed Cookies)** section and select **Yes Edit** to save

For additional information on using trusted signer process see https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-trusted-signers.html

PUBLIC S3 BUCKET: For distributions that are using a Public S3 bucket as an origin please ensure that the CloudFront distribution gets **account MD approval** and then raise a **false positive request** with InfoSec.

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.