Violation:

S3 buckets in your account are not enforcing HTTPS for web communications.

Description:

S3 buckets in your account are not enforcing HTTPS for web communications. HTTPS Ensures that your AWS S3 buckets enforce encryption of data over the network (as it travels to and from Amazon S3) using Secure Sockets Layer (SSL). Enforcing encryption and use of secure protocols help to ensure communications cannot be intercepted by unauthorized parties.

Instructions:

- Navigate to **S3** dashboard at https://console.aws.amazon.com/s3/.
- Select the S3 bucket that you want to encrypt and click the **Properties** tab from the dashboard top right menu.
- Inside the Properties tab, click **Permissions** to expand the bucket permissions settings panel.
- Click the **Edit** bucket policy button to edit the bucket policy in use. If the selected bucket does not have an access policy defined yet, click Add bucket policy.
- In the **Bucket Policy Editor** dialog box, perform one of the following actions based on your current configuration:
    1. If there is no access policy currently in use, paste the following policy document in the **Bucket Policy Editor** box, replace the bucket name, i.e. **DOC-EXAMPLE-BUCKET**, with the name of your own S3 bucket , click **Save**.
    2. This policy will restrict non-SSL S3 access to all your objects available in the selected S3 bucket. The policy will look like below.

```
{
"Id": "ExamplePolicy",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "AllowSSLRequestsOnly",
"Action": "s3:*",
"Effect": "Deny",
"Resource": [
"arn:aws:s3:::DOC-EXAMPLE-BUCKET",
"arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
],
"Condition": {
"Bool": {
"aws:SecureTransport": "false"
}
},
"Principal": "*"

}
]

}
```

3. If the selected bucket has already an access policy implemented, append any of below policies to the existing ones available within the **Bucket Policy Editor** box.

```
{
"Sid": "AllowSSLRequestsOnly",
"Action": "s3:*",
"Effect": "Deny",
"Resource": [
"arn:aws:s3:::DOC-EXAMPLE-BUCKET",
"arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
],
"Condition": {
"Bool": {
"aws:SecureTransport": "false"
}
},
"Principal": "*"

}
```

- **Ensure there are no permissions statements with Effect "Allow" when "aws:SecureTransport": "false" or Effect "Deny" when "aws:SecureTransport": "true".**

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.