

































-  Secrets
-  ABAP
-  Apex
-  C
-  C++
-  CloudFormation
-  COBOL
-  C#
-  CSS
-  Flex
-  Go
-  HTML
-  Java
-  JavaScript
-  Kotlin
-  Kubernetes
-  Objective C
-  PHP
-  PL/I
-  PL/SQL
-  Python
-  RPG
-  Ruby
-  Scala
-  Swift
-  Terraform
-  Text
-  TypeScript
-  T-SQL
-  VB.NET
-  VB6
-  XML



CloudFormation static code analysis













Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your CLOUDFORMATION code

All rules 27

 Vulnerability 3

 Security Hotspot 20

 Code Smell 4

Allowing public ACLs or policies on a S3 bucket is security-sensitive		Security Hotspot
Authorizing HTTP communications with S3 buckets is security-sensitive		Security Hotspot
Using clear-text protocols is security-sensitive		Security Hotspot
"Log Groups" should be configured with a retention policy		Code Smell
Defining a short backup retention duration is security-sensitive		Security Hotspot
Using unencrypted EFS file systems is security-sensitive		Security Hotspot
Using unencrypted SQS queues is security-sensitive		Security Hotspot
Using unencrypted SNS topics is security-sensitive		Security Hotspot
Using unencrypted SageMaker notebook instances is security-sensitive		Security Hotspot
Using unencrypted Elasticsearch domains is security-sensitive		Security Hotspot
Using unencrypted RDS databases is security-sensitive		Security Hotspot
Using unencrypted EBS volumes is security-sensitive		Security Hotspot

Tags

▼

Search by name...

🔍

Allowing public ACLs or policies on a S3 bucket is security-sensitive

Analyze your code

 Security Hotspot

 Critical



 aws cwe owasp

By default S3 buckets are private, it means that only the bucket owner can access it.

This access control can be relaxed with ACLs or policies.

To prevent permissive policies to be set on a S3 bucket the following settings can be configured:

- BlockPublicAcls: to block or not public ACLs to be set to the S3 bucket.
- IgnorePublicAcls: to consider or not existing public ACLs set to the S3 bucket.
- BlockPublicPolicy: to block or not public policies to be set to the S3 bucket.
- RestrictPublicBuckets: to restrict or not the access to the S3 endpoints of public policies to the principals within the bucket owner account.

Ask Yourself Whether

- The S3 bucket stores sensitive data.
- The S3 bucket is not used to store static resources of websites (images, css ...).
- Many users have the permission to set ACL or policy to the S3 bucket.
- These settings are not already enforced to true at the account level.

There is a risk if you answered yes to any of those questions.

Recommended Secure Coding Practices

It's recommended to configure:

- BlockPublicAcls to true to block new attempts to set public ACLs.
- IgnorePublicAcls to true to block existing public ACLs.
- BlockPublicPolicy to true to block new attempts to set public policies.
- RestrictPublicBuckets to true to restrict existing public policies.

Sensitive Code Example

By default, when not set, the PublicAccessBlockConfiguration is fully deactivated (nothing is blocked):

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucketdefault:
    Type: 'AWS::S3::Bucket' # Sensitive
    Properties:
      BucketName: "example"
```

This PublicAccessBlockConfiguration allows public ACL to be set:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket' # Sensitive
    Properties:
      BucketName: "example"
      PublicAccessBlockConfiguration:
        BlockPublicAcls: false # should be true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

Compliant Solution

This PublicAccessBlockConfiguration blocks public ACLs and policies, ignores existing public ACLs and restricts existing public policies:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket' # Compliant
    Properties:
      BucketName: "example"
      PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

See

- OWASP Top 10 2021 Category A1 - Broken Access Control
- OWASP Top 10 2021 Category A5 - Security Misconfiguration
- AWS Documentation - Blocking public access to your Amazon S3 storage
- MITRE, CWE-284 - Improper Access Control
- OWASP Top 10 2017 Category A5 - Broken Access Control

Available In:

sonarcloud



sonarqube

