


- 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

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
Disabling logging is security-sensitive
Security Hotspot
"Log Groups" should be declared explicitly
Code Smell

## Authorizing HTTP communications with S3 buckets is security-sensitive

Analyze your code

Security Hotspot

Critical

aws cwe owasp

By default, S3 buckets can be accessed through HTTP and HTTPs protocols.

Only HTTPs prevents data breaches by encrypting network communications.

### Ask Yourself Whether

- The S3 bucket stores sensitive information.
- The infrastructure needs to comply to some regulations, like HIPAA or PCI DSS, and other standards.

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

### Recommended Secure Coding Practices

It's recommended to deny all HTTP requests:

- for all objects (\*) of the bucket
- for all principals (\*)
- for all actions (\*)

### Sensitive Code Example

No secure policy is attached to this S3 bucket:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket' # Sensitive
```

A policy is defined but forces only HTTPs communication for some users:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket' # Sensitive
    Properties:
      BucketName: "mynoncompliantbucket"

  S3BucketPolicy:
    Type: 'AWS::S3::BucketPolicy'
    Properties:
      Bucket: !Ref S3Bucket
      PolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Deny
            Principal:
              AWS: # Sensitive: only one principal is forced to use https
                - 'arn:aws:iam::123456789123:root'
            Action: "*"
            Resource: arn:aws:s3:::mynoncompliantbuckets6249/*
            Condition:
              Bool:
                "aws:SecureTransport": false
```

### Compliant Solution

A secure policy that denies the use of all HTTP requests:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket' # Compliant
    Properties:
      BucketName: "mycompliantbucket"

  S3BucketPolicy:
    Type: 'AWS::S3::BucketPolicy'
    Properties:
      Bucket: "mycompliantbucket"
      PolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Deny
            Principal:
              AWS: "*" # all principals should use https
            Action: "*" # for any actions
            Resource: arn:aws:s3:::mycompliantbucket/* # for any resources
            Condition:
              Bool:
                "aws:SecureTransport": false
```

### See

- [OWASP Top 10 2021 Category A2](#) - Cryptographic Failures
- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration
- [AWS documentation](#) - Enforce encryption of data in transit
- [MITRE, CWE-319](#) - Cleartext Transmission of Sensitive Information
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration

Available In:

sonarcloud

sonarqube