

































-  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

Tags ▾

Search by name... 

 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
Administration services access should be restricted to specific IP addresses
 Vulnerability
Disabling versioning of S3 buckets is security-sensitive
 Security Hotspot
Disabling server-side encryption of S3 buckets is security-sensitive
 Security Hotspot
AWS tag keys should comply with a naming convention
 Code Smell
CloudFormation parsing failure
 Code Smell

Disabling versioning of S3 buckets is security-sensitive

Analyze your code

 Security Hotspot

 Minor ?

 [aws](#) [owasp](#)

S3 buckets can be in three states related to versioning:

- unversioned (default one)
- enabled
- suspended

When the S3 bucket is unversioned or has versioning suspended it means that a new version of an object overwrites an existing one in the S3 bucket.

It can lead to unintentional or intentional information loss.

Ask Yourself Whether

- The bucket stores information that require high availability.

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

Recommended Secure Coding Practices

It's recommended to enable S3 versioning and thus to have the possibility to retrieve and restore different versions of an object.

Sensitive Code Example

Versioning is disabled by default:

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

Compliant Solution

Versioning is enabled:

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket' # Compliant
    Properties:
      BucketName: "Example"
      VersioningConfiguration:
        Status: Enabled
```

See

- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration
- [AWS documentation](#) - Using versioning in S3 buckets
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration

Available In:

sonarcloud  | sonarqube 