



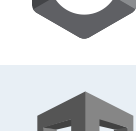


























-  Secrets
-  ABAP
-  Apex
-  C
-  C++
-  **CloudFormation**
-  COBOL
-  C#
-  CSS
-  Flex
-  Go
-  HTML
-  Java
-  JavaScript
-  Kotlin
-  Kubernetes
-  Objective C
-  PHP
-  RPG
-  Ruby
-  Scala
-  Swift
-  Terraform
-  Text
-  TypeScript
-  T-SQL
-  VB.NET
-  VB6
-  XML






# 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... 🔍

Creating public APIs is security-sensitive	 Security Hotspot
Allowing public network access to cloud resources is security-sensitive	 Security Hotspot
Having AWS policies that grant access to all resources of an account is security-sensitive	 Security Hotspot
Having policies that grant all privileges is	

## Creating public APIs is security-sensitive

[Analyze your code](#)

-  Security Hotspot
-  Blocker
- 
- 

A public API, which can be requested by any authenticated or unauthenticated identities, can lead to unauthorized actions and information disclosures.

### Ask Yourself Whether

The public API:

- exposes sensitive data like personal information.
- can be used to perform sensitive operations.
- is not protected by a security mechanism.
- answered yes to any of those questions.

### Noncompliant Coding Practices

It's recommended to restrict API access to authorized entities, unless the API offers a non-sensitive service designed to be public.

### Noncompliant Code Example

A public API that doesn't have access control implemented:

```
NoncompliantApiGatewayMethod:
  Type: AWS::ApiGateway::Method
  Properties:
    AuthorizationType: NONE # Sensitive
    HttpMethod: GET
```

A Serverless Application Model (SAM) API resource that is public by default:

```
OpenApiDefault: # Sensitive
Type: AWS::Serverless::Api
Properties:
  StageName: Prod
```

### Compliant Solution

An API that implements AWS IAM permissions:

```
MyApiGatewayMethodIam:
  Type: AWS::ApiGateway::Method
  Properties:
    AuthorizationType: AWS_IAM
    HttpMethod: GET
```

A Serverless Application Model (SAM) API resource that has to be requested using a key:


```
ApiKeyApi:
  Type: AWS::Serverless::Api
  Properties:
    StageName: Prod
    Auth:
      ApiKeyRequired: true
```

### See

- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [AWS Documentation](#) - Controlling and managing access to a REST API in API Gateway
- [MITRE, CWE-284](#) - Improper Access Control
- [OWASP Top 10 2017 Category A5](#) - Broken Access Control

Available In:

**sonarcloud**  | **sonarqube** 



SonarSource SA's websites use cookies to distinguish you from other users of our websites. This helps us to provide you with a good experience when you browse our websites and also allows us to improve them.