

































-  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... 

Having AWS policies that grant access to all resources of an account is security-sensitive		Security Hotspot
Having policies that grant all privileges is security-sensitive		Security Hotspot
Policies authorizing public access to resources are security-sensitive		Security Hotspot
Granting access to S3 buckets to all or authenticated users is security-sensitive		Security Hotspot
AWS IAM policies should not allow privilege escalation		Vulnerability
Weak SSL/TLS protocols should not be used		Vulnerability
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

Having AWS policies that grant access to all resources of an account is security-sensitive

Analyze your code

 Security Hotspot

 Blocker



 aws cwe owasp

A policy that allows identities to access all resources in an AWS account may violates [the principle of least privilege](#). Suppose an identity has permission to access all resources even though it only requires access to some non-sensitive ones. In this case, unauthorized access and disclosure of sensitive information will occur.

Ask Yourself Whether

The AWS account:

- has more than one resource with different levels of sensitivity.

There is a risk if you answered yes to any of this question.

Recommended Secure Coding Practices

It's recommended to apply the least privilege principle, i.e. by only granting access to necessary resources. A good practice to achieve this is to organize or [tag](#) resources depending on the sensitivity level of data they store or process. Therefore, managing a secure access control is less prone to errors.

Noncompliant Code Example

Update permission is granted for all policies using the wildcard (*) in the `Resource` property:

```
MyPolicy:
  Type: AWS::IAM::ManagedPolicy
  Properties:
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: Allow
          Action:
            - "iam:CreatePolicyVersion"
          Resource:
            - "*" # Sensitive

  Roles:
    - !Ref MyRole
```

Compliant Solution

Restrict update permission to the appropriate subset of policies:

```
MyPolicy:
  Type: AWS::IAM::ManagedPolicy
  Properties:
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Effect: Allow
          Action:
            - "iam:CreatePolicyVersion"
          Resource:
            - !Sub "arn:aws:iam::${AWS::AccountId}:policy/team1/*"

  Roles:
    - !Ref MyRole
```

Exceptions

No issue is reported when on Key policies in AWS KMS.

See

- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [AWS Documentation](#) - Grant least privilege
- [MITRE, CWE-732](#) - Incorrect Permission Assignment for Critical Resource
- [MITRE, CWE-284](#) - Improper Access Control
- [OWASP Top 10 2017 Category A5](#) - Broken Access Control

Available In:

sonarcloud  | **sonarqube** 