




Secrets


ABAP


Apex


C


C++


CloudFormation


COBOL


C#


CSS


Flex


Go


HTML


Java


JavaScript


Kotlin


Objective C


PHP


PL/I


PL/SQL


Python


RPG


Ruby


Scala


Swift


Terraform


Text


TypeScript

T-SQL

VB.NET

VB6


XML





## Terraform static code analysis

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

All rules 50

 Vulnerability 5


 Security Hotspot 43

 Code Smell 2


Tags ▾

Search by name... 🔍


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


Google Cloud load balancers SSL policies should not offer weak cipher suites

 Vulnerability


Azure custom roles should not grant subscription Owner capabilities

 Vulnerability

Excluding users or groups activities from audit logs is security-sensitive




 Security Hotspot

Defining a short log retention duration 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:

```
resource "aws_iam_policy" "noncompliantpolicy" {
  name = "noncompliantpolicy"


  policy = jsonencode({
    Version = "2012-10-17"
    Statement = [
      {
        Action = [
          "iam:CreatePolicyVersion"
        ]
        Effect = "Allow"
        Resource = [
          "*" # Sensitive
        ]
      }
    ]
  })
}
```

#### Compliant Solution


https://rules.sonarsource.com/terraform/RSPEC-6304

1/2


Enabling Attribute-Based Access Control for Kubernetes is security-sensitive

 Security Hotspot


Creating custom roles allowing privilege escalation is security-sensitive

 Security Hotspot

Creating App Engine handlers without requiring TLS is security-sensitive

 Security Hotspot

Excessive granting of GCP IAM permissions is security-sensitive

 Security Hotspot

Restrict update permission to the appropriate subset of policies:

```
resource "aws_iam_policy" "compliantpolicy" {
  name      = "compliantpolicy"

  policy = jsonencode({
    Version = "2012-10-17"
    Statement = [
      {
        Action = [
          "iam:CreatePolicyVersion"
        ]
        Effect   = "Allow"
        Resource = [
          "arn:aws:iam::${data.aws_caller_identity.current.account_id}:policy/*"
        ]
      }
    ]
  })
}
```

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:

