




 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... 


Defining a short log retention duration is security-sensitive

 Security Hotspot


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


Enabling project-wide SSH keys to access VM instances is security-sensitive

 Security Hotspot


Granting public access to GCP resources is security-sensitive

 Security Hotspot


Creating GCP SQL instances without requiring TLS is security-sensitive

 Security Hotspot


Creating DNS zones without DNSSEC enabled is security-sensitive

 Security Hotspot

Creating keys without a rotation period is security-sensitive




 Security Hotspot

Granting highly privileged GCP resource rights is security-sensitive

 Security Hotspot

Allowing public ACLs or policies on a S3 bucket is security-sensitive

Analyze your code

 Security Hotspot  Critical  aws cwe owasp

By default S3 buckets are private, it means that only the bucket owner can access it.

This access control can be relaxed with ACLs or policies.

To prevent permissive policies to be set on a S3 bucket the following settings can be configured:

- BlockPublicAcls: to block or not public ACLs to be set to the S3 bucket.
- IgnorePublicAcls: to consider or not existing public ACLs set to the S3 bucket.
- BlockPublicPolicy: to block or not public policies to be set to the S3 bucket.
- RestrictPublicBuckets: to restrict or not the access to the S3 endpoints of public policies to the principals within the bucket owner account.

Ask Yourself Whether

- The S3 bucket stores sensitive data.
- The S3 bucket is not used to store static resources of websites (images, css ...).
- Many users have the permission to set ACL or policy to the S3 bucket.
- These settings are not already enforced to true at the account level.

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

Recommended Secure Coding Practices

It's recommended to configure:

- BlockPublicAcls to true to block new attempts to set public ACLs.
- IgnorePublicAcls to true to block existing public ACLs.
- BlockPublicPolicy to true to block new attempts to set public policies.
- RestrictPublicBuckets to true to restrict existing public policies.

Sensitive Code Example

By default, when not set, the `aws_s3_bucket_public_access_block` is fully deactivated (nothing is blocked):

```
resource "aws_s3_bucket" "example" { # Sensitive: no Public bucket = "example" }
```

This `aws_s3_bucket_public_access_block` allows public ACL to be set:

```
resource "aws_s3_bucket" "example" { # Sensitive bucket = "examplename" }

resource "aws_s3_bucket_public_access_block" "example-publi
```


https://rules.sonarsource.com/terraform/RSPEC-6281

1/2

Using unencrypted cloud storages is security-sensitive

 Security Hotspot

Azure role assignments that grant access to all resources of a subscription are security-sensitive

 Security Hotspot

Disabling Role-Based Access Control on Azure resources is security-sensitive

 Security Hotspot

Disabling certificate-based authentication is security-sensitive

 Security Hotspot

```
bucket = aws_s3_bucket.example.id

block_public_acls      = false # should be true
block_public_policy    = true
ignore_public_acls     = true
restrict_public_buckets = true
}
```

Compliant Solution

This `aws_s3_bucket_public_access_block` blocks public ACLs and policies, ignores existing public ACLs and restricts existing public policies:

```
resource "aws_s3_bucket" "example" {
  bucket = "example"
}

resource "aws_s3_bucket_public_access_block" "example-publi
  bucket = aws_s3_bucket.example.id

  block_public_acls      = true
  block_public_policy    = true
  ignore_public_acls     = true
  restrict_public_buckets = true
}
```

See

- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration
- [AWS Documentation](#) - Blocking public access to your Amazon S3 storage
- [MITRE, CWE-284](#) - Improper Access Control
- [OWASP Top 10 2017 Category A5](#) - Broken Access Control

Available In:

