




 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... 


 Security Hotspot


Using unencrypted EFS file systems is security-sensitive




 Security Hotspot


Using unencrypted SQS queues is security-sensitive




 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

 Vulnerability

Administration services access should be restricted to specific IP addresses




 Security Hotspot

Unversioned Google Cloud Storage buckets are security-sensitive

 Vulnerability

Disabling S3 bucket MFA delete is security-sensitive

Unversioned Google Cloud Storage buckets are security-sensitive

 Security Hotspot  Minor  aws owasp

When object versioning for Google Cloud Storage (GCS) buckets is enabled, different versions of an object are stored in the bucket, preventing accidental deletion. A specific version can always be deleted when the generation number of an object version is specified in the request.

Object versioning cannot be enabled on a bucket with a retention policy. A retention policy ensures that an object is retained for a specific period of time even if a request is made to delete or replace it. Thus, a retention policy locks the single current version of an object in the bucket, which differs from object versioning where different versions of an object are retained.

Ask Yourself Whether

- The bucket stores information that require high availability.

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

Recommended Secure Coding Practices

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

Sensitive Code Example

Versioning is disabled by default:

```
resource "google_storage_bucket" "example" { # Sensitive Code Example
  name          = "example"
  location      = "US"
}
```

Compliant Solution

Versioning is enabled:

```
resource "google_storage_bucket" "example" {
  name          = "example"
  location      = "US"

  versioning {
    enabled = "true"
  }
}
```

See

- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration



https://rules.sonarsource.com/terraform/RSPEC-6412

1/2

| |
|--|
| Security Hotspot |
| 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 |
| Terraform parsing failure |
| Code Smell |

- [GCP documentation](#) - Object Versioning
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration

Available In:

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved. [Privacy Policy](#)