




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


 Security Hotspot


Disabling S3 bucket MFA delete is security-sensitive

Disabling versioning of S3 buckets is security-sensitive

Analyze your code

 Security Hotspot

 Minor ?

 aws owasp

S3 buckets can be in three states related to versioning:

- unversioned (default one)
- enabled
- suspended

When the S3 bucket is unversioned or has versioning suspended it means that a new version of an object overwrites an existing one in the S3 bucket.

It can lead to unintentional or intentional information loss.

Ask Yourself Whether

- The bucket stores information that require high availability.

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

Recommended Secure Coding Practices

It's recommended to enable S3 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 "aws_s3_bucket" "example" { # Sensitive
  bucket = "example"
}
```

Compliant Solution

Versioning is enabled:

```
resource "aws_s3_bucket" "example" { # Compliant
  bucket = "example"






  versioning {
    enabled = true
  }
}
```

See

- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration
- [AWS documentation](#) - Using versioning in S3 buckets
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration

https://rules.sonarsource.com/terraform/RSPEC-6252

1/2

<div> Security Hotspot</div>
<div><div>Disabling versioning of S3 buckets is security-sensitive</div><div> Security Hotspot</div></div>
<div><div>Disabling server-side encryption of S3 buckets is security-sensitive</div><div> Security Hotspot</div></div>
<div><div>AWS tag keys should comply with a naming convention</div><div> Code Smell</div></div>
<div><div>Terraform parsing failure</div><div> Code Smell</div></div>

Available In:

sonarcloud



|

sonarqube



© 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](#)