




 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 S3 bucket MFA delete is security-sensitive

Analyze your code

 Security Hotspot

 Minor ?

 cwe owasp

When S3 buckets versioning is enabled it's possible to add an additional authentication factor before being allowed to delete versions of an object or changing the versioning state of a bucket. It prevents accidental object deletion by forcing the user sending the delete request to prove that he has a valid MFA device and a corresponding valid token.

#### Ask Yourself Whether

- The S3 bucket stores sensitive information that is required to be preserved on the long term.
- The S3 bucket grants delete permission to many users.

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

#### Recommended Secure Coding Practices

It's recommended to enable S3 MFA delete, note that:

- MFA delete can only be enabled with the AWS CLI or API and with the root account.
- To delete an object version, the API should be used with the `x-amz-mfa` header.
- The API request, with the `x-amz-mfa` header, can only be used in HTTPS.

#### Sensitive Code Example

A versioned S3 bucket doesn't have MFA delete enabled:

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

  versioning {
    enabled = true
  }
}
```

#### Compliant Solution






MFA delete is enabled (**it's not possible to set this option** to a new S3 bucket with Terraform but the Terraform template can be updated that way it reflects the state):

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

  versioning {
    enabled = true
  }
}
```

https://rules.sonarsource.com/terraform/RSPEC-6255

1/2

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

```
mfa_delete = true
}
```

See

- [OWASP Top 10 2021 Category A7](#) - Identification and Authentication Failures
- [AWS documentation](#) - Configuring MFA delete
- [MITRE, CWE-308](#) - Use of Single-factor Authentication
- [OWASP Top 10 2017 Category A2](#) - Broken Authentication

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](#)