




 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

## Using unencrypted SQS queues is security-sensitive

 Security Hotspot  Major ?  aws cwe owasp

Amazon Simple Queue Service (SQS) is a managed message queuing service for application-to-application (A2A) communication. Amazon SQS can store messages encrypted as soon as they are received. In the case that adversaries gain physical access to the storage medium or otherwise leak a message from the file system, for example through a vulnerability in the service, they are not able to access the data.

### Ask Yourself Whether

- The queue contains sensitive data that could cause harm when leaked.
- There are compliance requirements for the service to store data encrypted.

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

### Recommended Secure Coding Practices

It's recommended to encrypt SQS queues that contain sensitive information. Encryption and decryption are handled transparently by SQS, so no further modifications to the application are necessary.

### Sensitive Code Example

For [aws\\_sqs\\_queue](#):

```
resource "aws_sqs_queue" "queue" { # Sensitive, encrypt
  name = "sqs-unencrypted"
}
```

### Compliant Solution

For [aws\\_sqs\\_queue](#):






```
resource "aws_sqs_queue" "queue" {
  name = "sqs-encrypted"
  kms_master_key_id = aws_kms_key.enc_key.key_id
}
```

### See

- [OWASP Top 10 2021 Category A2](#) - Cryptographic Failures
- [OWASP Top 10 2021 Category A4](#) - Insecure Design
- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration
- [Encryption at rest](#)
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration
- [MITRE, CWE-311](#) - Missing Encryption of Sensitive Data

https://rules.sonarsource.com/terraform/RSPEC-6330

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

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](#)