




 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




Using unencrypted SQS queues is security-sensitive




Using unencrypted SNS topics is security-sensitive




Using unencrypted SageMaker notebook instances is security-sensitive




Using unencrypted Elasticsearch domains is security-sensitive




Using unencrypted RDS databases is security-sensitive




Using unencrypted EBS volumes is security-sensitive




Disabling logging is security-sensitive




Administration services access should be restricted to specific IP addresses



Unversioned Google Cloud Storage buckets are security-sensitive



Disabling S3 bucket MFA delete is security-sensitive



Using unencrypted RDS databases is security-sensitive

Security Hotspot

Major ?

aws cwe owasp

Amazon Relational Database Service (RDS) allows to easily host and manage a relational database in the cloud. RDS databases can be encrypted, ensuring the security of data-at-rest. In the case that adversaries gain physical access to the storage medium they are not able to access the data.

Ask Yourself Whether

- The database 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 databases that contain sensitive information. Encryption and decryption are handled transparently by RDS, so no further modifications to the application are necessary.

Sensitive Code Example

For [aws_db_instance](#):

```
resource "aws_db_instance" "database" {
  storage_encrypted = false # Sensitive, disabled by d
}
```

Compliant Solution

For [aws_db_instance](#):






```
resource "aws_db_instance" "database" {
  storage_encrypted = true
}
```

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
- [Encrypting Amazon RDS resources](#)
- [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-6303

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:
sonardcloud  | **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](#)