




 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

Security Hotspot

Administration services access should be restricted to specific IP addresses

Vulnerability

Unversioned Google Cloud Storage buckets are security-sensitive

Security Hotspot

Disabling S3 bucket MFA delete is security-sensitive

Security Hotspot

Using unencrypted SageMaker notebook instances is security-sensitive

Analyze your code

Security Hotspot

Major ?

aws cwe owasp

Amazon SageMaker is a managed machine learning service in a hosted production-ready environment. To train machine learning models, SageMaker instances can process potentially sensitive data, such as personal information that should not be stored unencrypted. In the event that adversaries physically access the storage media, they cannot decrypt encrypted data.

Ask Yourself Whether

- The instance 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 SageMaker notebook instances that contain sensitive information. Encryption and decryption are handled transparently by SageMaker, so no further modifications to the application are necessary.

Sensitive Code Example

For `aws_sagemaker_notebook_instance`:

```
resource "aws_sagemaker_notebook_instance" "notebook" { # S
}
```

Compliant Solution



For `aws_sagemaker_notebook_instance`:

```
resource "aws_sagemaker_notebook_instance" "notebook" {
  kms_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
- [Protect Data at Rest Using Encryption](#)
- [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

Available In:

sonarcloud  sonarqube 

https://rules.sonarsource.com/terraform/RSPEC-6319

1/2

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