




 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

Creating keys without a rotation period is security-sensitive

 Security Hotspot  Major  gcp

The likelihood of security incidents increases when cryptographic keys are used for a long time. Thus, to strengthen the data protection it's recommended to rotate the symmetric keys created with the Google Cloud Key Management Service (KMS) automatically and periodically. Note that it's not possible in GCP KMS to rotate asymmetric keys automatically.

Ask Yourself Whether

- The cryptographic key is a symmetric key.
- The application requires compliance with some security standards like PCI-DSS.

Recommended Secure Coding Practices

It's recommended to rotate keys automatically and regularly. The shorter the key period, the less data can be decrypted by an attacker if a key is compromised. So the key rotation period usually depends on the amount of data encrypted with a key or other requirements such as compliance with security standards. In general, a period of time of 90 days can be used.

Sensitive Code Example

```
resource "google_kms_crypto_key" "noncompliant-key" { # Sensitive code
  name      = "crypto-key-compliant"
  key_ring  = google_kms_key_ring.keyring.id
}
```



Compliant Solution

```
resource "google_kms_crypto_key" "compliant-key" {
  name      = "crypto-key-compliant"
  key_ring  = google_kms_key_ring.keyring.id
  rotation_period = "7776000s" # 90 days
}
```

See

- [OWASP Top 10 2021 Category A2](#) - Cryptographic Failures
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration
- [GCP Documentation](#) - KMS Key rotation

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

1/2

https://rules.sonarsource.com/terraform/RSPEC-6401

Disabling versioning of S3 buckets is security-sensitive

 Security Hotspot

Disabling server-side encryption of S3 buckets is security-sensitive

 Security Hotspot

AWS tag keys should comply with a naming convention

 Code Smell

Terraform parsing failure

 Code Smell