




 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

Defining a short backup retention duration is security-sensitive

 Security Hotspot  Major ? 

Reducing the backup retention duration can reduce an organization's ability to re-establish service in case of a security incident.

Data backups allow to overcome corruption or unavailability of data by recovering as efficiently as possible from a security incident.

Backup retention duration, coverage, and backup locations are essential criteria regarding functional continuity.

Ask Yourself Whether

- This component is essential for the information system infrastructure.
- This component is essential for mission-critical functions.
- Compliance policies require this component to be backed up for a specific amount of time.

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

Recommended Secure Coding Practices

Increase the backup retention period to an amount of time sufficient enough to be able to restore service in case of an incident.

Sensitive Code Example

For [Amazon Relational Database Service](#) clusters and instances:

```
resource "aws_db_instance" "example" {
  backup_retention_period = 2 # Sensitive
}
```

For [Azure Cosmos DB](#) accounts:

```
resource "azurerm_cosmosdb_account" "example" {
  backup {
    type = "Periodic"
    retention_in_hours = 8 # Sensitive
  }
}
```






Compliant Solution

For [Amazon Relational Database Service](#) clusters and instances:

```
resource "aws_db_instance" "example" {
  backup_retention_period = 5
}
```

https://rules.sonarsource.com/terraform/RSPEC-6364

1/2

 Security Hotspot
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

For [Azure Cosmos DB](#) accounts:

```
resource "azurerm_cosmosdb_account" "example" {  
  backup {  
    type = "Periodic"  
    retention_in_hours = 300  
  }  
}
```

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](#)