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

Using unencrypted EBS volumes is security-sensitive

Analyze your code

Security Hotspot Major aws cwe owasp

Amazon Elastic Block Store (EBS) is a block-storage service for Amazon Elastic Compute Cloud (EC2). EBS volumes can be encrypted, ensuring the security of both data-at-rest and data-in-transit between an instance and its attached EBS storage. In the case that adversaries gain physical access to the storage medium they are not able to access the data. Encryption can be enabled for specific volumes or for all new volumes and snapshots.

Ask Yourself Whether

- The disk 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 EBS volumes that contain sensitive information. Encryption and decryption are handled transparently by EC2, so no further modifications to the application are necessary. Instead of enabling encryption for every volume it is also possible to enable encryption globally for a specific region.

Sensitive Code Example

For aws_ebs_volume:

```
resource "aws_ebs_volume" "ebs_volume" {  # Sensitive a
}
```

```
resource "aws_ebs_volume" "ebs_volume" {
  encrypted = false  # Sensitive
}
```

For aws_ebs_encryption_by_default:

```
resource "aws_ebs_encryption_by_default" "default_encry
  enabled = false  # Sensitive
}
```

For aws_launch_configuration:

```
resource "aws_launch_configuration" "launch_configurati
  root_block_device {  # Sensitive as encryption is dis
  }
  ebs_block_device {  # Sensitive as encryption is disa
```

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

```
  }
}
```

```
resource "aws_launch_configuration" "launch_configurati
  root_block_device {
    encrypted = false  # Sensitive
  }
  ebs_block_device {
    encrypted = false  # Sensitive
  }
}
```

Compliant Solution

For aws_ebs_volume:

```
resource "aws_ebs_volume" "ebs_volume" {
  encrypted = true
}
```

For aws_ebs_encryption_by_default:

```
resource "aws_ebs_encryption_by_default" "default_encry
  enabled = true  # Optional, default is "true"
}
```

For aws_launch_configuration:

```
resource "aws_launch_configuration" "launch_configurati
  root_block_device {
    encrypted = true
  }
  ebs_block_device {
    encrypted = true
  }
}
```

See

- OWASP Top 10 2021 Category A4 - Insecure Design
- OWASP Top 10 2021 Category A5 - Security Misconfiguration
- Amazon EBS 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