sonar RULES

Products

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

Granting public access to GCP resources is security-sensitive

Analyze your code

Security Hotspot Major gcp cwe-284

Granting public access to GCP resources may reduce an organization's ability to protect itself against attacks or theft of its GCP resources.
Security incidents associated with misuse of public access include disruption of critical functions, data theft, and additional costs due to resource overload.

To be as prepared as possible in the event of a security incident, authentication combined with fine-grained permissions helps maintain the principle of defense in depth and trace incidents back to the perpetrators.

GCP also provides the ability to grant access to a large group of people:

- If public access is granted to all Google users, the impact of a data theft is the same as if public access is granted to all Internet users.
- If access is granted to a large Google group, the impact of a data theft is limited based on the size of the group.

The only thing that changes in these cases is the ability to track user access in the event of an incident.

Ask Yourself Whether

- This GCP resource is essential to the information system infrastructure.
- This GCP resource is essential to mission-critical functions.
- This GCP resource stores or processes sensitive data.
- Compliance policies require that access to this resource be authenticated.

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

Recommended Secure Coding Practices

Explicitly set access to this resource or function as private.

Sensitive Code Example

For IAM resources:

```
resource "google_cloudfunctions_function_iam_binding" "
  members = [
    "allUsers",              # Sensitive
    "allAuthenticatedUsers", # Sensitive
  ]
}

resource "google_cloudfunctions_function_iam_member" "e
  member = "allAuthenticatedUsers" # Sensitive
}
```

For ACL resources:

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 "google_storage_bucket_access_control" "exampl
  entity = "allUsers" # Sensitive
}

resource "google_storage_bucket_acl" "example" {
  role_entity = [
    "READER:allUsers",              # Sensitive
    "READER:allAuthenticatedUsers", # Sensitive
  ]
}
```

For container clusters:

```
resource "google_container_cluster" "example" {
  private_cluster_config {
    enable_private_nodes    = false # Sensitive
    enable_private_endpoint = false # Sensitive
  }
}
```

Compliant Solution

For IAM resources:

```
resource "google_cloudfunctions_function_iam_binding" "
  members = [
    "serviceAccount:${google_service_account.example.em
    "group:${var.example_group}"
  ]
}

resource "google_cloudfunctions_function_iam_member" "e
  member = "user:${var.example_user}" # Sensitive
}
```

For ACL resources:

```
resource "google_storage_bucket_access_control" "exampl
  entity = "user-${var.example_user]"
}

resource "google_storage_bucket_acl" "example" {
  role_entity = [
    "READER:user-name@example.com",
    "READER:group-admins@example.com"
  ]
}
```

For container clusters:

```
resource "google_container_cluster" "example" {
  private_cluster_config {
    enable_private_nodes    = true
    enable_private_endpoint = true
  }
}
```

See

- OWASP Top 10 2021 Category A1 - Boken Access Control
- OWASP Top 10 2017 Category A5 - Broken Access Control
- MITRE, CWE-668 - Exposure of Resource to Wrong Sphere

Available In:

sonarcloud sonarqube