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...

Enabling Azure resource-specific admin accounts is security-sensitive
Security Hotspot

Disabling Managed Identities for Azure resources is security-sensitive
Security Hotspot

Assigning high privileges Azure Active Directory built-in roles is security-sensitive
Security Hotspot

Defining a short backup retention duration is security-sensitive
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

Creating App Engine handlers without requiring TLS is security-sensitive

Analyze your code

Security Hotspot Major gcp

App Engine supports encryption in transit through TLS. As soon as the app is deployed, it can be requested using `appspot.com` domains or custom domains. By default, endpoints accept both clear-text and encrypted traffic. When communication isn't encrypted, there is a risk that an attacker could intercept it and read confidential information.

When creating an App Engine, request handlers can be set with different security level for encryption:

- `SECURE_NEVER`: only HTTP requests are allowed (HTTPS requests are redirected to HTTP).
- `SECURE_OPTIONAL` and `SECURE_DEFAULT`: both HTTP and HTTPS requests are allowed.
- `SECURE_ALWAYS`: only HTTPS requests are allowed (HTTP requests are redirected to HTTPS).

Ask Yourself Whether

- The handler serves confidential data in HTTP responses.

There is a risk if you answered yes to this question.

Recommended Secure Coding Practices

It's recommended for App Engine handlers to require TLS for all traffic. It can be achieved by setting the security level to `SECURE_ALWAYS`.

Sensitive Code Example

`SECURE_DEFAULT`, `SECURE_NEVER` and `SECURE_OPTIONAL` are sensitive TLS security level:

```
resource "google_app_engine_standard_app_version" "exam
  version_id = "v1"
  service    = "default"
  runtime    = "nodejs"

  handlers {
    url_regex                   = ".*"
    redirect_http_response_code = "REDIRECT_HTTP_RESPON
    security_level              = "SECURE_OPTIONAL" # S
    script {
      script_path = "auto"
    }
  }
}
```

Compliant Solution

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

Disabling versioning of S3 buckets is

Force the use of TLS for the handler by setting the security level on `SECURE_ALWAYS`:

```
resource "google_app_engine_standard_app_version" "exam
  version_id = "v1"
  service    = "default"
  runtime    = "nodejs"

  handlers {
    url_regex                   = ".*"
    redirect_http_response_code = "REDIRECT_HTTP_RESPON
    security_level              = "SECURE_ALWAYS"
    script {
      script_path = "auto"
    }
  }
}
```

See

- OWASP Top 10 2021 Category A2 - Cryptographic Failures
- OWASP Top 10 2017 Category A3 - Sensitive Data Exposure
- OWASP Top 10 2017 Category A6 - Security Misconfiguration
- MITRE, CWE-200 - Exposure of Sensitive Information to an Unauthorized Actor
- MITRE, CWE-319 - Cleartext Transmission of Sensitive Information
- GCP Documentation - Overview of App Security

Available In:

sonarcloud sonarqube