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...

sensitive

Security Hotspot

Disabling certificate-based authentication is security-sensitive

Security Hotspot

Assigning high privileges Azure Resource Manager built-in roles is security-sensitive

Security Hotspot

Authorizing anonymous access to Azure resources is security-sensitive

Security Hotspot

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

Enabling Attribute-Based Access Control for Kubernetes is security-sensitive

Analyze your code

Security Hotspot Major cwe owasp gcp

Enabling Legacy Authorization, Attribute-Based Access Control (ABAC), on Google Kubernetes Engine resources can reduce an organization's ability to protect itself against access controls being compromised.

For Kubernetes, Attribute-Based Access Control has been superseded by Role-Based Access Control. ABAC is not under active development anymore and thus should be avoided.

Ask Yourself Whether

- This resource is essential for the information system infrastructure.
- This resource is essential for mission-critical functions.
- Compliance policies require access to this resource to be enforced through the use of Role-Based Access Control.

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

Recommended Secure Coding Practices

Unless you are relying on ABAC, leave it disabled.

Sensitive Code Example

For Google Kubernetes Engine:

```
resource "google_container_cluster" "example" {
  enable_legacy_abac = true # Sensitive
}
```

Compliant Solution

For Google Kubernetes Engine:

```
resource "google_container_cluster" "example" {
  enable_legacy_abac = false
}
```

See

- OWASP Top 10 2021 Category A1 - Boken Access Control
- OWASP Top 10 2017 Category A5 - Boken Access Control
- MITRE, CWE-668 - Exposure of Resource to Wrong Sphere
- Google Cloud Documentation - Hardening your cluster's security

Available In:

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

sonarcloud sonarqube

Privacy Policy