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

Disabling Role-Based Access Control on Azure resources is security-sensitive

Analyze your code

Security Hotspot Major cwe owasp azure

Disabling Role-Based Access Control (RBAC) on Azure resources can reduce an organization's ability to protect itself against access controls being compromised.

To be considered safe, access controls must follow the principle of least privilege and correctly segregate duties amongst users. RBAC helps enforce these practices by adapting the organization's access control needs into explicit role-based policies: It helps keeping access controls maintainable and sustainable.

Furthermore, RBAC allows operations teams to work faster during a security incident. It helps to mitigate account theft or intrusions by quickly shutting down accesses.

Ask Yourself Whether

- This Azure resource is essential for the information system infrastructure.
- This Azure 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

- Enable Azure RBAC when the Azure resource supports it.
- For Kubernetes clusters, enable Azure RBAC if Azure AD integration is supported. Otherwise, use the built-in Kubernetes RBAC.

Sensitive Code Example

For Azure Kubernetes Services:

```
resource "azurerm_kubernetes_cluster" "example" {
  role_based_access_control {
    enabled = false # Sensitive
  }
}

resource "azurerm_kubernetes_cluster" "example2" {
  role_based_access_control {
    enabled = true

    azure_active_directory {
      managed = true
      azure_rbac_enabled = false # Sensitive
    }
```

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 Key Vaults:

```
resource "azurerm_key_vault" "example" {
  enable_rbac_authorization = false # Sensitive

}
```

Compliant Solution

For Azure Kubernetes Services:

```
resource "azurerm_kubernetes_cluster" "example" {
  role_based_access_control {
    enabled = true
  }
}

resource "azurerm_kubernetes_cluster" "example" {
  role_based_access_control {
    enabled = true

    azure_active_directory {
      managed = true
      azure_rbac_enabled = true
    }
  }
}
```

For Key Vaults:

```
resource "azurerm_key_vault" "example" {
  enable_rbac_authorization   = 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