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...

Azure role assignments that grant access to all resources of a subscription are security-sensitive

Security Hotspot

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

Defining a short log retention duration is security-sensitive

Analyze your code

Security Hotspot Major azure gcp

Defining a short log retention duration can reduce an organization’s ability to backtrace the actions of malicious actors in case of a security incident.

Logging allows operational and security teams to get detailed and real-time feedback on an information system’s events. The logging coverage enables them to quickly react to events, ranging from the most benign bugs to the most impactful security incidents, such as intrusions.

Apart from security detection, logging capabilities also directly influence future digital forensic analyses. For example, detailed logging will allow investigators to establish a timeline of the actions perpetrated by an attacker.

Ask Yourself Whether

- This component is essential for the information system infrastructure.
- This component is essential for mission-critical functions.
- Compliance policies require traceability for a longer duration.

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

Recommended Secure Coding Practices

Setting log retention period to 14 days is the bare minimum. It’s recommended to increase it to 30 days or above.

Sensitive Code Example

For Azure Firewall Policy:

```
resource "azurerm_firewall_policy" "example" {
  insights {
    enabled = true
    retention_in_days = 7 # Sensitive
  }
}
```

For Google Cloud Logging buckets:

```
resource "google_logging_project_bucket_config" "exampl
    project = var.project
    location = "global"
    retention_days = 7 # Sensitive
    bucket_id = "_Default"
}
```

Compliant Solution

For Azure Firewall Policy:

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

```
resource "azurerm_firewall_policy" "example" {
  insights {
    enabled = true
    retention_in_days = 30
  }
}
```

For Google Cloud Logging buckets:

```
resource "google_logging_project_bucket_config" "exampl
    project = var.project
    location = "global"
    retention_days = 30
    bucket_id = "_Default"
}
```

Available In:

sonarcloud sonarqube