




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... 

Creating DNS zones without DNSSEC enabled is security-sensitive

Security Hotspot

Creating keys without a rotation period is security-sensitive

Security Hotspot

Granting highly privileged GCP resource rights is security-sensitive

Security Hotspot

Using unencrypted cloud storages is security-sensitive

Security Hotspot

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

Azure custom roles should not grant subscription Owner capabilities

Analyze your code

Vulnerability

Major 

azure

Azure Resource Manager allows creating custom roles that can be assigned to users, groups, or service principals. A custom role that grants access to all resources of a subscription will have the same capabilities as the built-in Owner role.

It's recommended to limit the number of subscription owners in order to mitigate the risk of being breached by a compromised owner. Having a custom role that grants subscription Owner capabilities makes it way more difficult to enforce this limitation.

This rule raises an issue when a custom role has an assignable scope set to a Subscription or a Management Group and allows all actions (*)

Recommended Secure Coding Practices

- Apply the least privilege principle by creating a custom role with as few permissions as possible.
- As custom role can be updated, gradually add atomic permissions when required.
- Limit the assignable scopes of the custom role to a set of Resources or Ressource Groups.
- When necessary, use the built-in Owner role instead of a custom role granting subscription owner capabilities.
- Limit the assignments of Owner roles to less than three people or service principals.

Sensitive Code Example

```
resource "azurerm_role_definition" "example" { # Sensitive
  name      = "example"
  scope     = data.azurem_subscription.primary.id

  permissions {
    actions      = ["*"]
    not_actions = []
  }






  assignable_scopes = [
    data.azurem_subscription.primary.id
  ]
}
```

Compliant Solution

```
resource "azurerm_role_definition" "example" {
  name      = "example"
  scope     = data.azurem_subscription.primary.id
```

https://rules.sonarsource.com/terraform/RSPEC-6385

1/2

 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

```
permissions {
  actions      = ["Microsoft.Compute/*"]
  not_actions = []
}

assignable_scopes = [
  data.azurerm_subscription.primary.id
]
```

See

- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [OWASP Top 10 2021 Category A4](#) - Insecure Design
- [OWASP Top 10 2017 Category A5](#) - Broken Access Control
- [MITRE, CWE-266](#) - Incorrect Privilege Assignment
- [Azure Documentation](#) - Azure custom roles
- [Azure Documentation](#) - Best practices for Azure RBAC

Available In:

