




 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... 

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

Using unencrypted SageMaker notebook instances is security-sensitive







Security Hotspot

Using unencrypted Elasticsearch domains is security-sensitive



Security Hotspot

Creating custom roles allowing privilege escalation is security-sensitive

 Security Hotspot  Major   gcp cwe-284

Creating custom roles that allow privilege escalation can allow attackers to maliciously exploit an organization's cloud resources.

Certain GCP permissions allow impersonation of one or more privileged principals within a GCP infrastructure. To prevent privilege escalation after an account has been compromised, proactively follow GCP Security Insights and ensure that custom roles contain as few privileges as possible that allow direct or indirect impersonation.

For example, privileges like `deploymentmanager.deployments.create` allow impersonation of service accounts, even if the name does not sound like it. Other privileges like `setIamPolicy`, which are more explicit, directly allow their holder to extend their privileges.

After gaining a foothold in the target infrastructure, sophisticated attackers typically map their newfound roles to understand what is exploitable.

The riskiest privileges are either:





- At the infrastructure level: privileges to perform project, folder, or organization-wide administrative tasks.
- At the resource level: privileges to perform resource-wide administrative tasks.

In either case, the following privileges should be avoided or granted only with caution:

- `..setIamPolicy`
- `cloudbuilds.builds.create`
- `cloudfunctions.functions.create`
- `cloudfunctions.functions.update`
- `cloudscheduler.jobs.create`
- `composer.environments.create`
- `compute.instances.create`
- `dataflow.jobs.create`
- `dataproc.clusters.create`
- `deploymentmanager.deployments.create`
- `iam.roles.update`
- `iam.serviceAccountKeys.create`
- `iam.serviceAccounts.actAs`
- `iam.serviceAccounts.getAccessToken`
- `iam.serviceAccounts.getOpenIdToken`
- `iam.serviceAccounts.implicitDelegation`
- `iam.serviceAccounts.signBlob`
- `iam.serviceAccounts.signJwt`
- `orgpolicy.policy.set`
- `run.services.create`
- `serviceusage.apiKeys.create`
- `serviceusage.apiKeys.list`

https://rules.sonarsource.com/terraform/RSPEC-6408

1/3

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

- storage.hmacKeys.create

Ask Yourself Whether

- This role requires impersonation to perform specific tasks with different privileges.
- This custom role is intended for a small group of administrators.

There is a risk if you answered no to these questions.

Recommended Secure Coding Practices

Use a permission that does not allow privilege escalation.

Sensitive Code Example

Lightweight custom role intended for a developer:

```
resource "google_organization_iam_custom_role" "example" {
  permissions = [
    "iam.serviceAccounts.getAccessToken",      # Sensitive
    "iam.serviceAccounts.getOpenIdToken",      # Sensitive
    "iam.serviceAccounts.actAs",               # Sensitive
    "iam.serviceAccounts.implicitDelegation",  # Sensitive
    "resourceManager.projects.get",
    "resourceManager.projects.list",
    "run.services.create",
    "run.services.delete",
    "run.services.get",
    "run.services.getIamPolicy",
    "run.services.list",
    "run.services.update",
  ]
}
```

Lightweight custom role intended for a read-only user:

```
resource "google_project_iam_custom_role" "example" {
  permissions = [
    "iam.serviceAccountKeys.create",      # Sensitive
    "iam.serviceAccountKeys.get",         # Sensitive
    "deploymentManager.deployments.create", # Sensitive
    "cloudbuild.builds.create",           # Sensitive
    "resourceManager.projects.get",
    "resourceManager.projects.list",
    "run.services.get",
    "run.services.getIamPolicy",
    "run.services.list",
  ]
}
```

Compliant Solution

Lightweight custom role intended for a developer:

```
resource "google_project_iam_custom_role" "example" {
  permissions = [
    "resourceManager.projects.get",
    "resourceManager.projects.list",
    "run.services.create",
    "run.services.delete",
    "run.services.get",
    "run.services.getIamPolicy",
    "run.services.list",
    "run.services.update",
  ]
}
```

Lightweight custom role intended for a read-only user:

```
resource "google_project_iam_custom_role" "example" {
  permissions = [
    "resourceManager.projects.get",
    "resourceManager.projects.list",
  ]
}
```

```
"run.services.get",  
"run.services.getIamPolicy",  
"run.services.list",  
]  
}
```

See

- [GCP IAM Docs](#) - Support levels for permissions in custom roles
- [GCP IAM Docs](#) - Understanding IAM custom roles
- [DEFONConference Youtube Video](#) - DEF CON Safe Mode - Dylan Ayrey and Allison Donovan - Lateral Movement & Privilege Escalation in GCP
- [Rhino Security Labs](#) - Privilege Escalation in Google Cloud Platform - Part 1 (IAM)
- [Rhino Security Labs](#) - Privilege Escalation in Google Cloud Platform - Part 2 (Non-IAM)
- [Praetorian](#) - Google Cloud Platform (GCP) Service Account-based Privilege Escalation paths
- [GCP Docs](#) - Security Insights
- [OWASP Top 10 2021 Category A1](#) - Broken Access Control
- [OWASP Top 10 2017 Category A5](#) - Broken Access Control
- [MITRE, CWE-668](#) - Exposure of Resource to Wrong Sphere

Available In:

sonarcloud  **sonarqube** 

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.
[Privacy Policy](#)