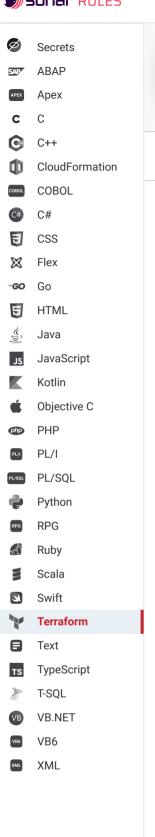
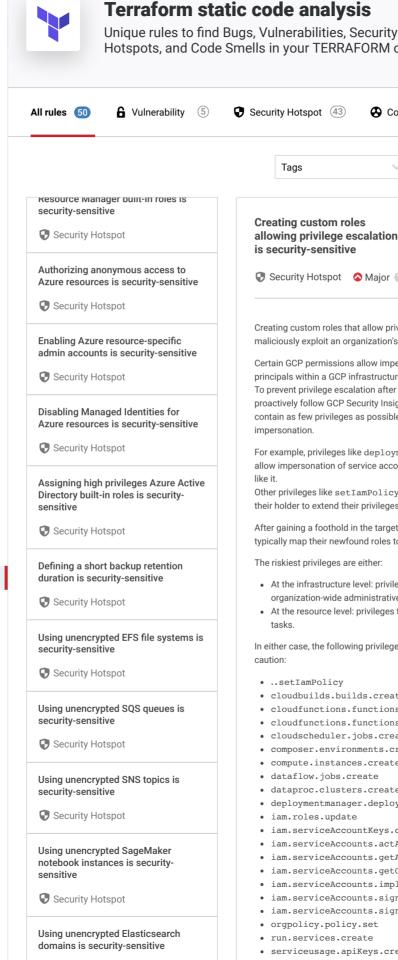
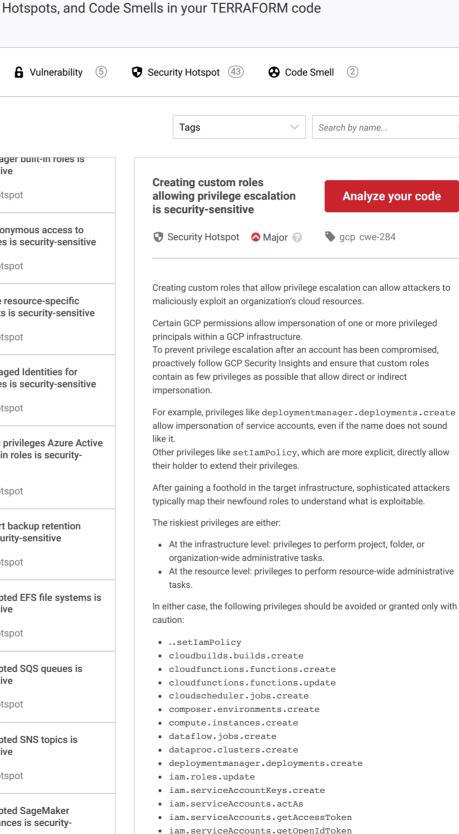


Products >







iam.serviceAccounts.implicitDelegation

• iam.serviceAccounts.signBlob • iam.serviceAccounts.signJwt • orgpolicy.policy.set

serviceusage.apiKeys.create • serviceusage.apiKeys.list

• run.services.create

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

6 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",
                                             # Sensiti
    "iam.serviceAccounts.getOpenIdToken",
                                             # Sensiti
   "iam.serviceAccounts.actAs",
                                             # Sensiti
   "iam.serviceAccounts.implicitDelegation", # Sensiti
    "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
 (IAM)
- Rhino Security Labs
 Privilege Escalation in Google Cloud Platform Part
 (Non-IAM)
- Praetorian Google Cloud Platform (GCP) Service Account-based Privilege Escalation paths
- GCP Docs Security Insights
- 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

© 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