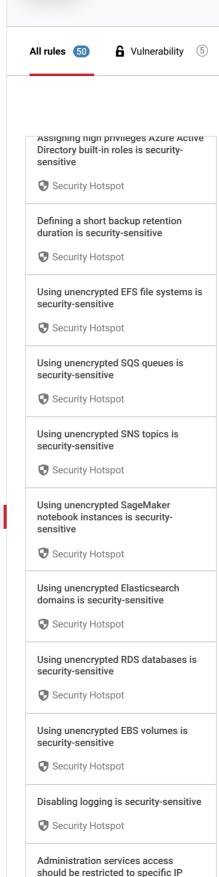
Terraform static code analysis

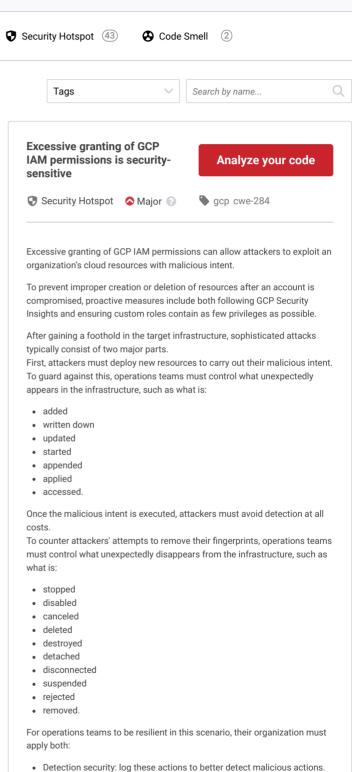
Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your TERRAFORM code



Products ∨







· Preventive security: review and limit granted permissions.

given parameter

Ask Yourself Whether

This rule raises an issue when a custom role grants a number of sensitive

permissions (read-write or destructive permission) that is greater than a

This custom role will be mostly used for read-only purposes.

Compliance policies require read-only access.

addresses

6 Vulnerability

Unversioned Google Cloud Storage buckets are security-sensitive

Security Hotspot

Disabling S3 bucket MFA delete is security-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

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

Recommended Secure Coding Practices

To reduce the risks associated with this role after a compromise:

- Reduce the list of permissions to grant only those that are actually needed
- Favor read-only over read-write.

Sensitive Code Example

This custom role grants more than 5 sensitive permissions:

```
resource "google_project_iam_custom_role" "example" {
  permissions = [ # Sensitive
      "resourcemanager.projects.create", # Sensitive perm
      "resourcemanager.projects.delete", # Sensitive perm
      "resourcemanager.projects.get",
      "resourcemanager.projects.list",
      "run.services.create", # Sensitive permission
      "run.services.delete", # Sensitive permission
      "run.services.get",
      "run.services.getTamPolicy",
      "run.services.setTamPolicy", # Sensitive permissio
      "run.services.list",
      "run.services.update", # Sensitive permission
]
}
```

Compliant Solution

This custom role grants less than 5 sensitive permissions:

```
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",
    ]
}
```

See

- GCP Docs Enforce least privilege with role recommendations
- 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