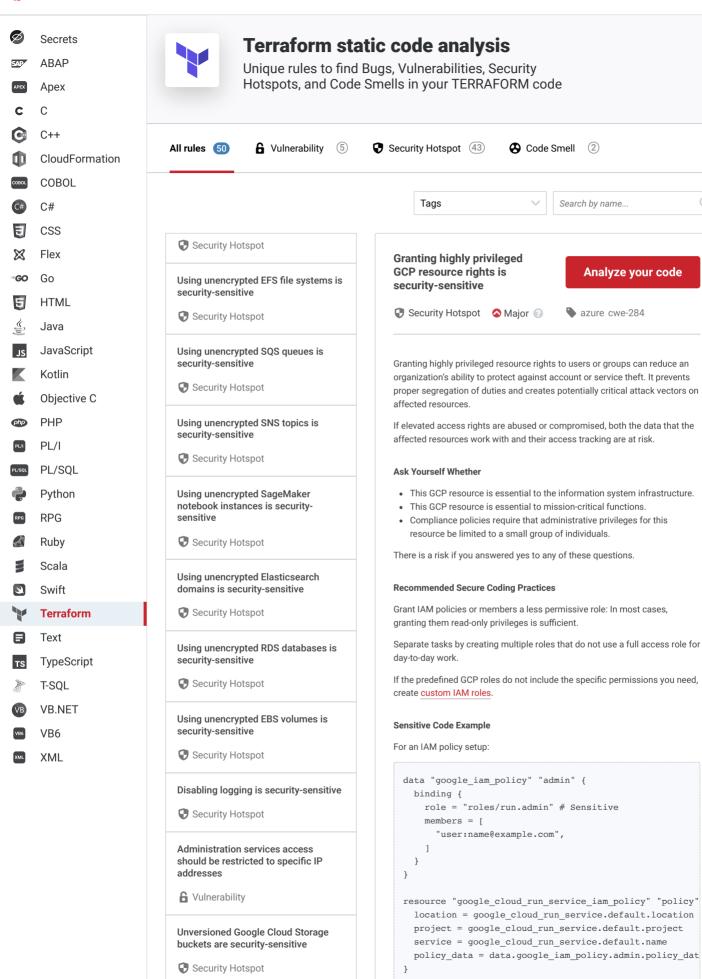


Products ∨



Disabling S3 bucket MFA delete is

security-sensitive

For an IAM policy binding:

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 naming convention

Code Smell

Terraform parsing failure

Code Smell

```
resource "google_cloud_run_service_iam_binding" "exampl
  location = google_cloud_run_service.default.location
  project = google_cloud_run_service.default.project
  service = google_cloud_run_service.default.name
  role = "roles/run.admin" # Sensitive
  members = [
    "user:name@example.com",
  ]
}
```

For adding a member to a policy:

```
resource "google_cloud_run_service_iam_member" "example
  location = google_cloud_run_service.default.location
  project = google_cloud_run_service.default.project
  service = google_cloud_run_service.default.name
  role = "roles/run.admin" # Sensitive
  member = "user:name@example.com"
}
```

Compliant Solution

For an IAM policy setup:

```
data "google_iam_policy" "admin" {
  binding {
    role = "roles/viewer"
    members = [
        "user:name@example.com",
    ]
  }
}

resource "google_cloud_run_service_iam_policy" "example
  location = google_cloud_run_service.default.location
  project = google_cloud_run_service.default.project
  service = google_cloud_run_service.default.name
  policy_data = data.google_iam_policy.admin.policy_dat
}
```

For an IAM policy binding:

```
resource "google_cloud_run_service_iam_binding" "exampl
  location = google_cloud_run_service.default.location
  project = google_cloud_run_service.default.project
  service = google_cloud_run_service.default.name
  role = "roles/viewer"
  members = [
    "user:name@example.com",
  ]
}
```

For adding a member to a policy:

```
resource "google_cloud_run_service_iam_member" "example
  location = google_cloud_run_service.default.location
  project = google_cloud_run_service.default.project
  service = google_cloud_run_service.default.name
  role = "roles/viewer"
  member = "user:name@example.com"
}
```

See

- OWASP Top 10 2021 Category A1 Broken Access Control
- OWASP Top 10 2017 Category A5 Broken Access Control
- MITRE, CWE-284 Improper Access Control

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