




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... 


Granting public access to GCP resources is security-sensitive

 Security Hotspot


Creating GCP SQL instances without requiring TLS is security-sensitive

 Security Hotspot


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

Excluding users or groups activities from audit logs is security-sensitive

Analyze your code

 Security Hotspot

 Major 

 gcp

The Google Cloud audit logs service records administrative activities and accesses to Google Cloud resources of the project. It's important to enable audit logs to be able to investigate malicious activities in the event of a security incident.

Some project members may be exempted from having their activities recorded in the Google Cloud audit log service, creating a blind spot and reducing the capacity to investigate future security events.

Ask Yourself Whether

- The members exempted from having their activity logged have high privileges.
- Compliance rules require that audit log should be activated for all members.

Recommended Secure Coding Practices

It is recommended to have a consistent audit logging policy for all project members and therefore not to create logging exemptions for certain members.

Sensitive Code Example






```
resource "google_project_iam_audit_config" "example" {
  project = data.google_project.project.id
  service = "allServices"
  audit_log_config {
    log_type = "ADMIN_READ"
    exempted_members = [ # Sensitive
      "user:rogue.administrator@gmail.com",
    ]
  }
}
```

Compliant Solution

```
resource "google_project_iam_audit_config" "example" {
  project = data.google_project.project.id
  service = "allServices"
  audit_log_config {
    log_type = "ADMIN_READ"
  }
}
```

https://rules.sonarsource.com/terraform/RSPEC-6414

1/2

 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

See

- [OWASP Top 10 2021 Category A9](#) - Security Logging and Monitoring Failures
- [OWASP Top 10 2017 Category A10](#) - Insufficient Logging & Monitoring
- [GCP Documentation](#) - Cloud Audit Logs overview

Available In:



© 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](#)