




 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

Google Cloud load balancers SSL policies should not offer weak cipher suites

Analyze your code

 Vulnerability

 Major ?

 cwe gcp owasp

TLS configuration of Google Cloud load balancers is defined through SSL policies. There are three managed profiles to choose from: COMPATIBLE (default), MODERN and RESTRICTED:

- The RESTRICTED profile relies only on secure cipher suites and should be used by applications that require to comply with the highest security standards.
- The MODERN profile includes additional cipher suites that present security weaknesses like using the SHA1 algorithm for signing.
- The COMPATIBLE profile offers the most common cipher suites and thus broader compatibility. Some of these use SHA1 or 3DES algorithms which are considered weak. Also, this profile includes cipher suites that rely on obsolete key-exchange mechanisms that don't provide forward secrecy[\[https://en.wikipedia.org/wiki/Forward\\_secrecy\]](https://en.wikipedia.org/wiki/Forward_secrecy) as a feature.

Noncompliant Code Example

```
resource "google_compute_ssl_policy" "example" {
  name           = "example"
  min_tls_version = "TLS_1_2"
  profile        = "COMPATIBLE" # Noncompliant
}
```




Compliant Solution

```
resource "google_compute_ssl_policy" "example" {
  name           = "example"
  min_tls_version = "TLS_1_2"
  profile        = "RESTRICTED"
}
```

See






- [OWASP Top 10 2021 Category A2](#) - Cryptographic Failures
- [OWASP Top 10 2021 Category A5](#) - Security Misconfiguration
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure
- [OWASP Top 10 2017 Category A6](#) - Security Misconfiguration
- [MITRE, CWE-327](#) - Use of a Broken or Risky Cryptographic Algorithm
- [SSL and TLS Deployment Best Practices](#) - Use Secure Cipher Suites
- [Google Cloud Load Balancing](#) - Defining an SSL policy

Available In:

https://rules.sonarsource.com/terraform/RSPEC-6410

1/2

 Security Hotspot
<b>Enabling Azure resource-specific admin accounts is security-sensitive</b>  Security Hotspot
<b>Disabling Managed Identities for Azure resources is security-sensitive</b>  Security Hotspot
<b>Assigning high privileges Azure Active Directory built-in roles is security-sensitive</b>  Security Hotspot
<b>Defining a short backup retention duration is security-sensitive</b>  Security Hotspot

© 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](#)