

































-  **Secrets**
-  ABAP
-  Apex
-  C
-  C++
-  CloudFormation
-  COBOL
-  C#
-  CSS
-  Flex
-  Go
-  HTML
-  Java
-  JavaScript
-  Kotlin
-  Kubernetes
-  Objective C
-  PHP
-  PL/I
-  PL/SQL
-  Python
-  RPG
-  Ruby
-  Scala
-  Swift
-  Terraform
-  Text
-  TypeScript
-  T-SQL
-  VB.NET
-  VB6
-  XML










## Secrets static code analysis

Unique rules to find Vulnerabilities in your source code and language agnostic config files

All rules 7  Vulnerability 

Tags ▾

Search by name... 

|   |
|---|
| Amazon Web Services credentials should not be disclosed<br> Vulnerability      |
| Amazon MWS credentials should not be disclosed<br> Vulnerability               |
| Google API keys should not be disclosed<br> Vulnerability                    |
| Google Cloud service accounts keys should not be disclosed<br> Vulnerability |
| Alibaba Cloud AccessKeys should not be disclosed<br> Vulnerability           |
| IBM API keys should not be disclosed<br> Vulnerability                       |
| Azure Storage Account Keys should not be disclosed<br> Vulnerability         |

### Google Cloud service accounts keys should not be disclosed

Analyze your code

 Vulnerability  Blocker   cwe sans-top25-porous owasp-a3

Google Cloud service accounts are designed to authenticate and authorize requests to Google APIs.

If your application interacts with Google Cloud services then it requires a service account to access all the resources it needs to function properly. Resources that can be accessed depend on the permission granted to the service account. Establishing the identity of a service account relies on a public/private key pair. It's common for private keys to be distributed through a JSON file that your application will then use to consume Google APIs.

A key may authenticate to a high privilege which has unrestricted access to all resources in your Google Cloud project, including billing information.

#### Recommended Secure Coding Practices

Only administrators should have access to the service account key used by your application.

As a consequence, service account keys should not be stored along with the application code as they would grant special privileges to anyone who has access to the application source code.

Keys should be stored outside of the code in a file that is never committed to your application code repository.

If possible, a better alternative is to use your cloud provider's service for managing secrets. On Google Cloud this service is called Secret Manager.

When keys are disclosed in the application code, consider them as compromised and revoke them immediately.

#### See

- [Google Cloud](#) - Creating and managing service account keys
- [OWASP Top 10 2017 Category A3](#) - Sensitive Data Exposure
- [MITRE, CWE-798](#) - Use of Hard-coded Credentials
- [MITRE, CWE-259](#) - Use of Hard-coded Password
- [CERT, MSC03-J](#) - Never hard code sensitive information
- [SANS Top 25](#) - Porous Defenses

Available In:

**sonarlint** 