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 7

Tags

Search by name...

Amazon Web Services credentials should not be disclosed
Vulnerability

Amazon MWS credentials should not be disclosed
Vulnerability

Google API keys should not be disclosed
Vulnerability

Google Cloud service accounts keys should not be disclosed
Vulnerability

Alibaba Cloud AccessKeys should not be disclosed
Vulnerability

IBM API keys should not be disclosed
Vulnerability

Azure Storage Account Keys should not be disclosed
Vulnerability

Azure Storage Account Keys should not be disclosed

Analyze your code

Vulnerability Blocker cwe sans-top25-porous owasp-a3

Azure Storage Account Keys are similar to the root password, allowing full access to Azure Storage Accounts.

If the application interacts with Azure Cloud Storage services, access keys should be secured and not be disclosed.

Recommended Secure Coding Practices

Only administrators should have access to storage account keys. To authorize an application to access an Azure Storage, it's recommended to createa service principal and assign it the required privileges only. AzureIdentity SDK provides several options such as *DefaultAzureCredential* that can be used to retrieve secrets from, for instance, environmentvariables.

Storage account keys should not be stored with the application code or saved anywhere in plain text accessible to others. Consider using an Azure Key Vault to store and manage keys.

When credentials are disclosed in the application code, consider them as compromised and rotate them immediately.

See

- docs.microsoft.com - Manage storage account access 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