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

Docker static code analysis

Unique rules to find Vulnerabilities, Security Hotspots, and Code Smells in your DOCKER code

All rules 44 | Vulnerability 4 | Bug 4 | Security Hotspot 15 | Code Smell 21

Tags | Impact | Clean code attribute | Search by name...

Specific version tag for image should be used
Code Smell

Package update should not be executed without installing it
Code Smell

Cache should be cleaned after package installation
Code Smell

Deprecated instructions should not be used
Code Smell

Consent flag should be set to avoid manual input
Code Smell

Environment variables should not be unset on a different layer than they were set
Code Smell

Expanded filenames should not become options
Code Smell

Double quote to prevent globbing and word splitting
Code Smell

Instructions should be upper case
Code Smell

Allowing non-root users to modify resources copied to an image is security-sensitive
Security Hotspot

Automatically installing recommended packages is security-sensitive
Security Hotspot

Specific version tag for image should be used

Analyze your code

Intentionality - Logical | Maintainability

Code Smell | Major

When a Dockerfile image is not tagged with a specific version, it is referred to as `latest`. This means that every time the image is built, deployed, or run, it will always use the latest version of the image.

Why is this an issue? | How can I fix it? | More Info

While using always the latest version may seem convenient, the build cannot be repeated because it is not clear which was the last version. In addition, it can lead to unpredictability and issues such as version mismatch and potential security vulnerabilities.

What is the potential impact?

For example, if a developer builds and deploys an application using `my-image:latest`, they may unknowingly be using a different version of the image than another developer who also built and deployed the same application using `my-image:latest`. This can lead to version mismatches, which can cause bugs or compatibility issues.

In addition, using `latest` as the tag for Dockerfile images can potentially introduce security vulnerabilities. For instance, if a security vulnerability is discovered in an image and a new version is released to fix it, using `latest` as the tag means that the application will automatically use the updated image, even if it has not been properly tested and vetted for compatibility with the application.

Available In:
sonarlint | sonarcloud | sonarqube