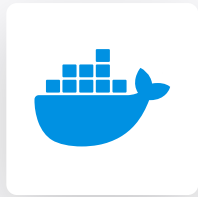


- Secrets
- ABAP
- Apex
- AzureResourceManager
- C
- C#
- C++
- CloudFormation
- COBOL
- COBOL
- CSS
- Dart
- Docker**
- Flex
- Go
- HTML
- Java
- JavaScript
- JCL
- JCL
- Kotlin
- Kubernetes
- Objective C
- PHP
- PL/I
- PL/SQL
- Python
- RPG
- RPG
- Ruby
- Scala
- Swift
- Terraform
- Text
- TypeScript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

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
Running containers as a privileged user is security-sensitive	Security Hotspot
Delivering code in production with debug features activated is security-sensitive	Security Hotspot
Use ADD instruction to retrieve remote resources	Code Smell

Deprecated instructions should not be used

- Consistency - Conventional
- Maintainability ⬆
- Code Smell
- Major ?

Deprecated instructions should be replaced by other suggested instructions.

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

Code examples

Noncompliant code example

```
MAINTAINER bob
```

Compliant solution

```
LABEL org.opencontainers.image.authors="bob"
```

How does this work?

The LABEL instruction is much more flexible than MAINTAINER and should be used instead.

Available In:
sonarlint | **sonarcloud** | **sonarqube**

Analyze your code

