







































-  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 rules44

 Vulnerability4

 Bug4

 Security Hotspot15

 Code Smell21


Tags

Impact

Clean code attribute


Search by name...

Setting loose POSIX file permissions is security-sensitive




Security Hotspot

Reduce the amount of consecutive RUN instructions




Code Smell

Prefer COPY over ADD for copying local resources




Code Smell

WORKDIR instruction should only be used with absolute path




Code Smell

Too long RUN instruction should be split into multiple lines




Code Smell

Prefer Exec form for ENTRYPOINT and CMD instructions




Code Smell

"WORKDIR" instruction should be used instead of "cd" commands




Code Smell

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


## Setting loose POSIX file permissions is security-sensitive


Analyze your code

Consistency - Conventional

Security

 Security Hotspot

 Major

 cwe docker

In Unix file system permissions, the "others" category refers to all users except the owner of the file system resource and the members of the group assigned to this resource.

Granting permissions to this category can lead to unintended access to files or directories that could allow attackers to obtain sensitive information, disrupt services or elevate privileges.

Ask Yourself Whether

- The container is designed to be a multi-user environment.
- Services are run by dedicated low-privileged users to achieve privileges separation.

There is a risk if you answered yes to any of those questions.

Recommended Secure Coding Practices

The most restrictive possible permissions should be assigned to files and directories.

To be secure, remove the unnecessary permissions. If required, use `--chown` to set the target user and group.

Sensitive Code Example

```
# Sensitive
ADD --chmod=777 src dst
# Sensitive
COPY --chmod=777 src dst
# Sensitive
RUN chmod +x resource
# Sensitive
RUN chmod u+s resource
```

Compliant Solution

```
ADD --chmod=754 src dst
COPY --chown=user:user --chmod=744 src dst
RUN chmod u+x resource
RUN chmod +t resource
```

See

- CWE - [CWE-732 - Incorrect Permission Assignment for Critical Resource](#)
- [ADD](#) - Docker ADD command
- [COPY](#) - Docker COPY command
- [chmod reference](#) - chmod command
- [chown reference](#) - chown command
- STIG Viewer - [Application Security and Development: V-222430](#) - The application must execute without excessive account permissions.

Available In:

sonarlint

sonarcloud

sonarqube

© 2008-2024 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE, and SON are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.

Sonar helps developers write Clean Code.[Privacy Policy](#) | [Cookie Policy](#)

