




 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... 🔍


Using host operating system namespaces is security-sensitive

 Security Hotspot


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


## Using host operating system namespaces is security-sensitive


Analyze your code

Intentionality - Complete

Security ⬆

 Security Hotspot

 Major ⓘ

 docker cwe

Using host operating system namespaces can lead to compromise of the host system. Opening network services of the local host system to the container creates a new attack surface for attackers.

Host network sharing could provide a significant performance advantage for workloads that require critical network performance. However, the successful exploitation of this attack vector could have a catastrophic impact on confidentiality within the host.

Ask Yourself Whether

- The host exposes sensitive network services.
- The container’s services performances do **not** rely on operating system namespaces.

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

Recommended Secure Coding Practices

Do not use host operating system namespaces.

Sensitive Code Example

```
# syntax=docker/dockerfile:1.3
FROM example
# Sensitive
RUN --network=host wget -O /home/sessions http://127.0.0.1:9000/sessions
```

Compliant Solution

```
# syntax=docker/dockerfile:1.3
FROM example
RUN --network=none wget -O /home/sessions http://127.0.0.1:9000/sessions
```

See

- [Dockerfile reference](#) - Custom Dockerfile syntax
- [Dockerfile reference](#) - RUN --network
- CWE - [CWE-653 - Improper Isolation or Compartmentalization](#)

Available In:

sonarlint

sonarcloud

sonarqube

© 2008-2024 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE, and SONARWAVE 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](#)

