

Secrets

**ABAP** 



AzureResourceManager

**C** 0

C# C#

C++

CloudFormation

DBOL COBOL

CSS

Dart

Docker

💢 Flex

**©** Go

HTML

Js JavaScript

Java

JCL JCL

Kotlin

Kubernetes

Objective C

PPP PHP

PL/I PL/

PL/SQL

Ruby

**Python** 

RPG RPG

\_

Swif

Terraform

**Text** 

TypeScript

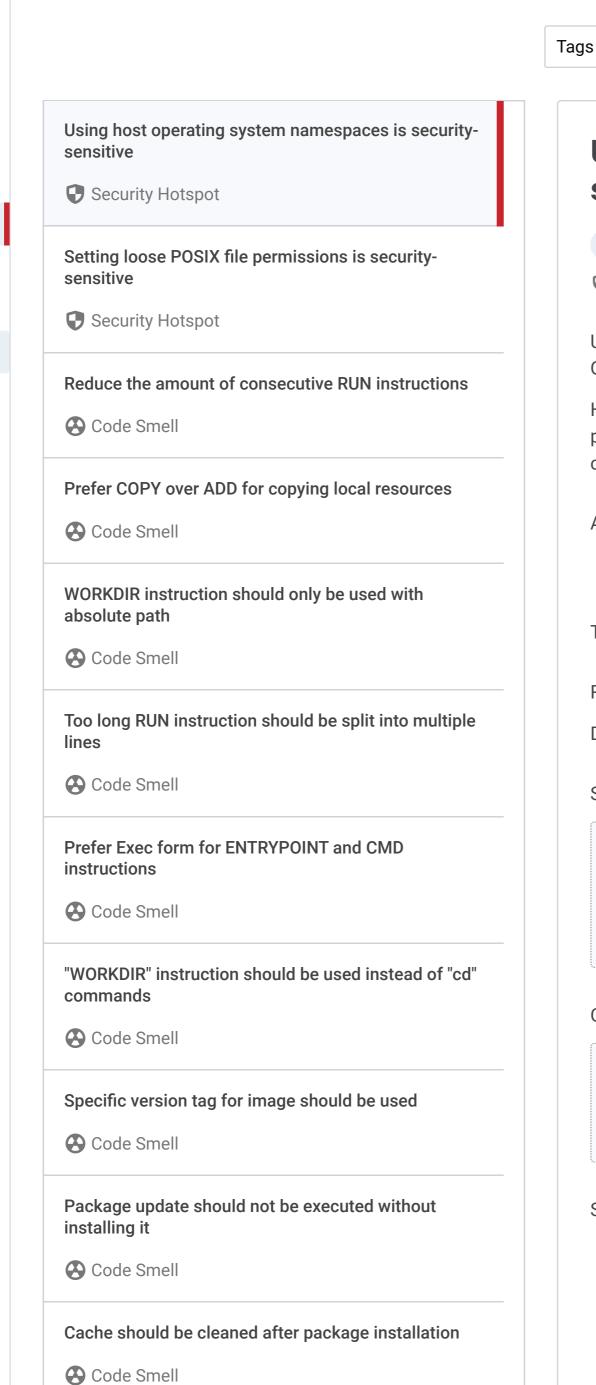
T-SQL

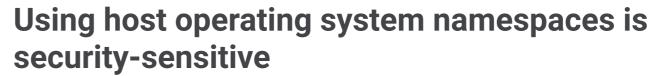
VB VB.NET

XML XML

## **Docker static code analysis**

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





Analyze your code

Search by name...

Intentionality - Complete Security Security Security Hotspot Major Odocker cwe

**Impact** 

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.

Clean code attribute

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 -0 /home/sessions http://127.0.0.1:9000/sessions

Compliant Solution

# syntax=docker/dockerfile:1.3

FROM example

RUN --network=none wget -0 /home/sessions http://127.0.0.1:9000/sessions

See

- <u>Dockerfile reference</u> Custom Dockerfile syntax
- Dockerfile reference RUN --network
- CWE CWE-653 Improper Isolation or Compartmentalization

Available In:

sonarlint ⊕ | sonarcloud ↔ | sonarqube

