



SAP ABAP

Apex

AzureResourceManager

C

C# C#

C++

CloudFormation

COBOL COBOL

CSS

Dart

Docker

DOCK

Flex

GO Go

⊎ HTML

🖺 Java

Js JavaScript

JCL JCL

Kotlin

Kubernetes

Objective C

DHP

PL/SQL

Python

RPG RPG

Ruby

SWIII

Terraform

Text

TS TypeScript

T-SQL

VB VB.NET

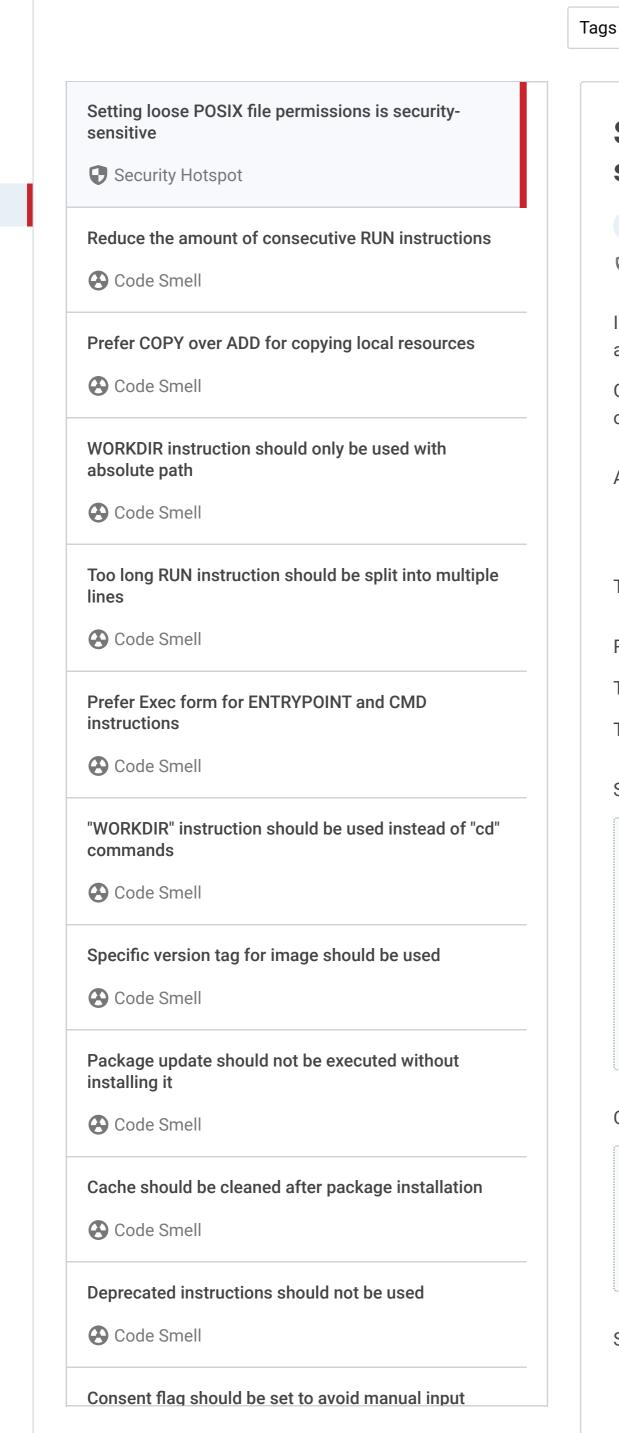
VB6 VB6

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...

Consistency - Conventional Security △

Security △

Security △

Security △

Consistency - Conventional Security △

Security △

Security △

Impact

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.

Clean code attribute

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 <u>Application Security and Development: V-222430</u> The application must execute without excessive account permissions.

Available In:

sonarlint ⊕ | sonarcloud む | sonarqube

