sonar RULES

Products

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...

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

Arguments in long RUN instructions should be sorted
Code Smell

Track uses of "TODO" tags
Code Smell

Descriptive labels are mandatory
Code Smell

Use digest to pin versions of base images
Code Smell

Dockerfile parsing failure
Code Smell

Pulling an image based on its digest is security-sensitive
Security Hotspot

Use digest to pin versions of base images

Analyze your code

Consistency - Conventional | Maintainability | Reliability | Security

Code Smell | Major

In Dockerfiles, it is recommended to use digests to pin versions of base images. This practice ensures that you are always using the exact version of the base image that you intend to use, making your Docker image builds reproducible.

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

Documentation

- Docker Docs - Building best practices

Available In:
sonarlint | sonarcloud | sonarqube