Q



AzureResourceManager

CloudFormation

COBOL

Docker

JavaScript

Kubernetes

Objective C

PL/SQL

**RPG** 

Terraform

Text

TypeScript

T-SQL

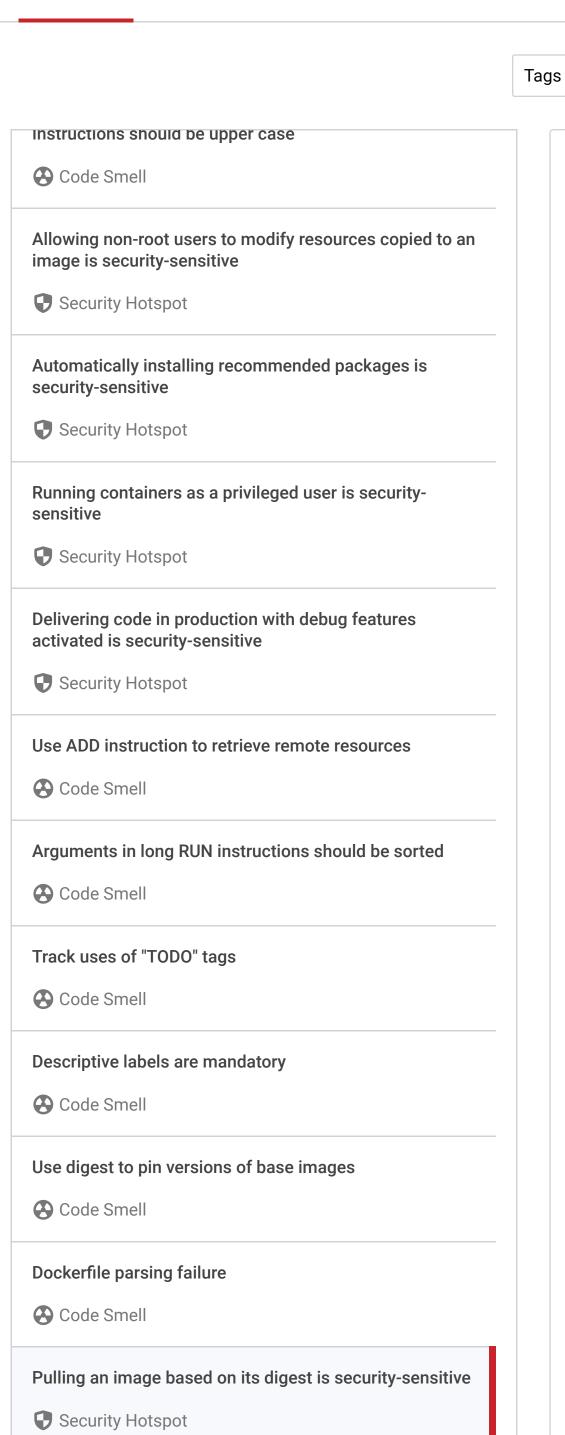
## **Docker static code analysis**

**G** Vulnerability

All rules 44

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

🛣 Bug



## Pulling an image based on its digest is security-sensitive

Clean code attribute

**Analyze your code** 

This rule is deprecated; use \$6596 instead. A container image digest uniquely and immutably identifies a container image. A tag, on the other hand, is a mutable reference to a container image.

This tag can be updated to point to another version of the container at any point in time.

dockerfile cwe

In general, the use of image digests instead of tags is intended to keep determinism stable within a system or infrastructure for reliability reasons.

The problem is that pulling such an image prevents the resulting container from being updated or patched in order to remove vulnerabilities or significant bugs.

Search by name..

Ask Yourself Whether

Security Hotspot (15)

You expect to receive security updates of the base image.

Code Smell (21)

**Impact** 

Responsibility - Trustworthy Security V

There is a risk if you answer yes to this question.

**Recommended Secure Coding Practices** 

Containers should get the latest security updates. If there is a need for determinism, the solution is to find tags that are not as prone to change as latest or shared tags.

To do so, favor a more precise tag that uses semantic versioning and target a major version, for example.

Sensitive Code Example

FROM mongo@sha256:8eb8f46e22f5ccf1feb7f0831d02032b187781b178cb971cd1222556a6cee9d1

RUN echo ls

**Compliant Solution** 

Here, mongo:6.0 is better than using a digest, and better than using a more precise version, such as 6.0.4, because it would prevent 6.0.5 security updates:

FROM mongo: 6.0

RUN echo ls

See

- Docker-Lock
- Skaffold, kpt, digester, kustomize, gke-deploy, ko, and Bazel
- GKE, Using Container Image Digests
- OpenShift, Builds and Image Streams

Available In:





