Search by name...



Secrets

Apex

AzureResourceManager

CloudFormation

**COBOL** 

**Docker** 

HTML

Java

**JavaScript** 

Kubernetes

Objective C

PL/SQL

**RPG** 

Ruby

Terraform

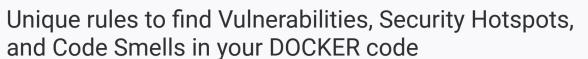
Text

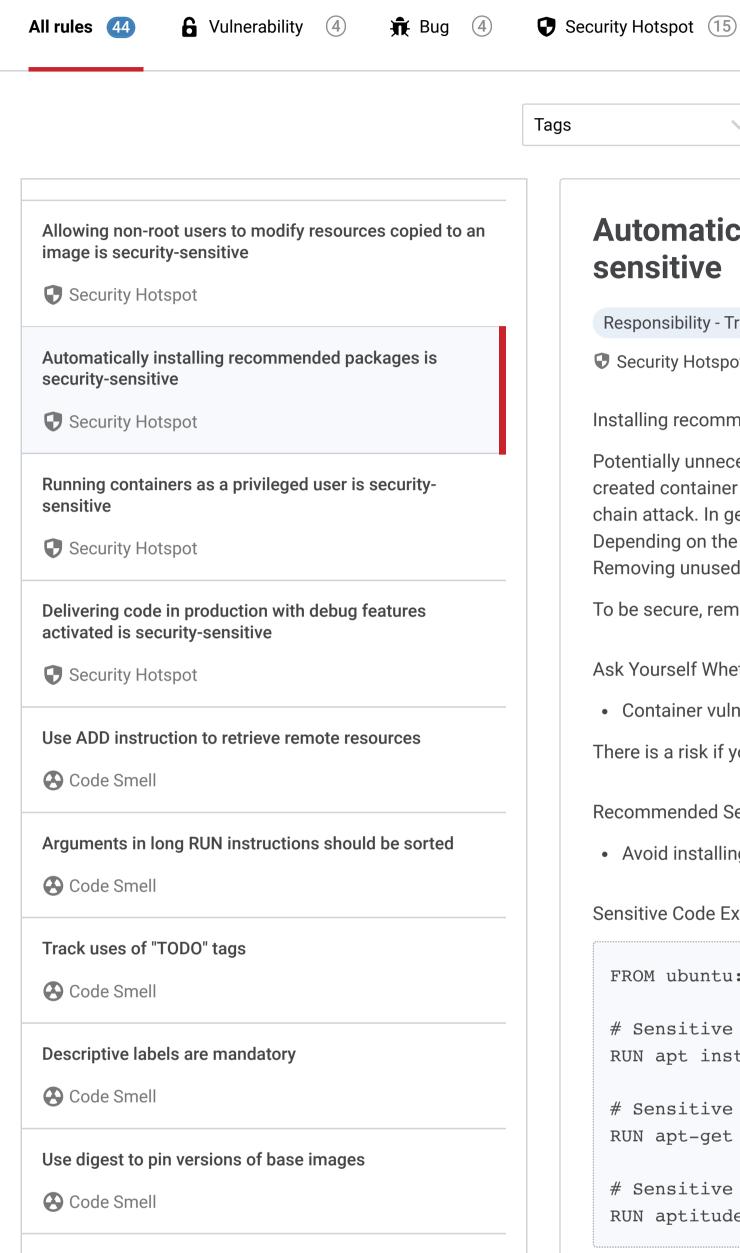
TypeScript

T-SQL

**VB.NET** 

## **Docker static code analysis**





Dockerfile parsing failure

Pulling an image based on its digest is security-sensitive

Code Smell

Security Hotspot



Clean code attribute

Analyze your code

Q

dockerfile

Responsibility - Trustworthy Security V

**Impact** 

Code Smell (21)

Installing recommended packages automatically can lead to vulnerabilities in the Docker image.

Potentially unnecessary packages are installed via a known Debian package manager. These packages will increase the attack surface of the created container as they might contain unidentified vulnerabilities or malicious code. Those packages could be used as part of a broader supply chain attack. In general, the more packages are installed in a container, the weaker its security posture is. Depending on the introduced vulnerabilities, a malicious actor accessing such a container could use these for privilege escalation.

Removing unused packages can also significantly reduce your Docker image size.

To be secure, remove unused packages where possible and ensure images are subject to routine vulnerability scans.

Ask Yourself Whether

· Container vulnerability scans are not performed.

There is a risk if you answered yes to the question.

**Recommended Secure Coding Practices** 

Avoid installing package dependencies that are not strictly required.

Sensitive Code Example

# Sensitive RUN apt install -y build-essential

FROM ubuntu:22.04

# Sensitive

RUN apt-get install -y build-essential

# Sensitive

RUN aptitude install -y build-essential

**Compliant Solution** 

FROM ubuntu:22.04

RUN apt --no-install-recommends install -y build-essential

RUN apt-get --no-install-recommends install -y build-essential

RUN aptitude --without-recommends install -y build-essential

See

• Debian Documentation - Binary Dependencies

• Ubuntu Blog - Container size reduction

Available In:



