

Secrets

ABAP

Apex

AzureResourceManager

CloudFormation

COBOL

CSS

Dart

Docker

HTML

Java

JavaScript

Kotlin

Kubernetes

Objective C

PL/SQL

PL/I

Python

RPG

Swift

Terraform

Text

TypeScript

T-SQL

VB.NET

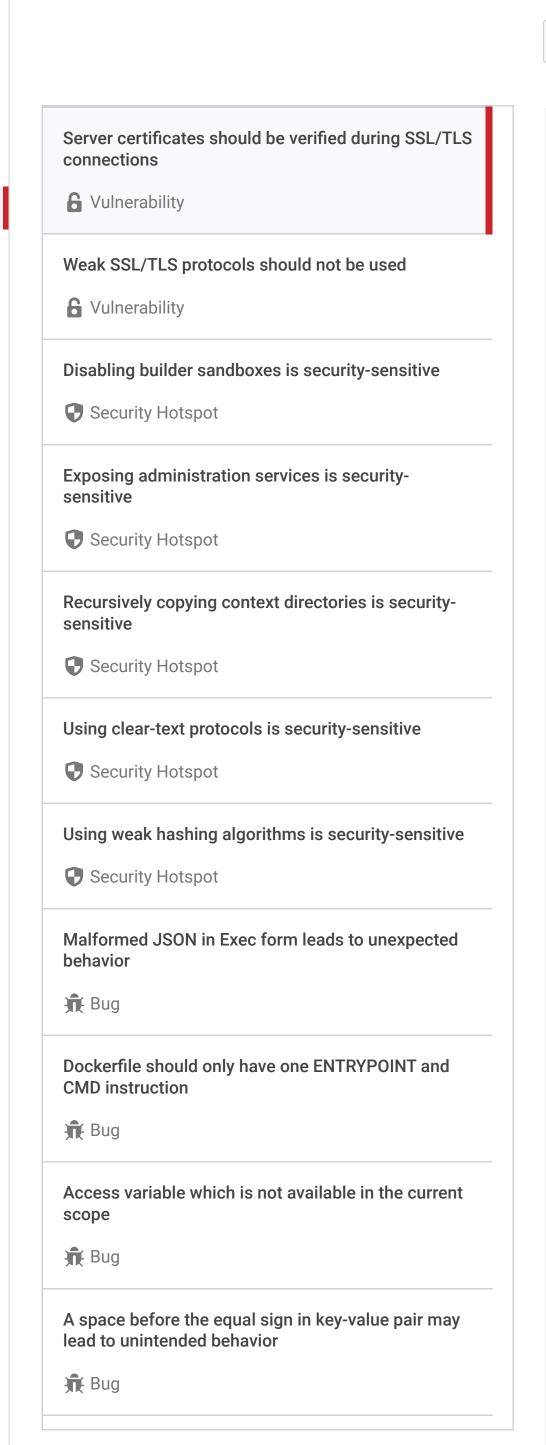


Docker static code analysis

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



Tags





Analyze your code

Search by name..

Responsibility - Trustworthy Security (2) **6** Vulnerability **6** Critical **9** cwe privacy ssl

Impact

This vulnerability makes it possible that an encrypted communication is intercepted.

Clean code attribute

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

Code examples

The following code contains examples of disabled certificate validation.

Noncompliant code example

FROM ubuntu:22.04 # Noncompliant RUN curl --insecure -0 https://expired.example.com/downloads/install.sh

Compliant solution

FROM ubuntu:22.04 RUN curl -0 https://new.example.com/downloads/install.sh

How does this work?

Addressing the vulnerability of disabled TLS certificate validation primarily involves re-enabling the default validation.

To avoid running into problems with invalid certificates, consider the following sections.

Using trusted certificates

If possible, always use a certificate issued by a well-known, trusted CA for your server. Most programming environments come with a predefined list of trusted root CAs, and certificates issued by these authorities are validated automatically. This is the best practice, and it requires no additional code or configuration.

Working with self-signed certificates or non-standard CAs

In some cases, you might need to work with a server using a self-signed certificate, or a certificate issued by a CA not included in your trusted roots. Rather than disabling certificate validation in your code, you can add the necessary certificates to your trust store.

Available In:

