

CloudFormation COBOL

CSS Dart

Docker

HTML Java

JavaScript

Kotlin

Kubernetes

Objective C

PL/I

PL/SQL

Python

RPG

Terraform

Swift

Text

TypeScript

T-SQL

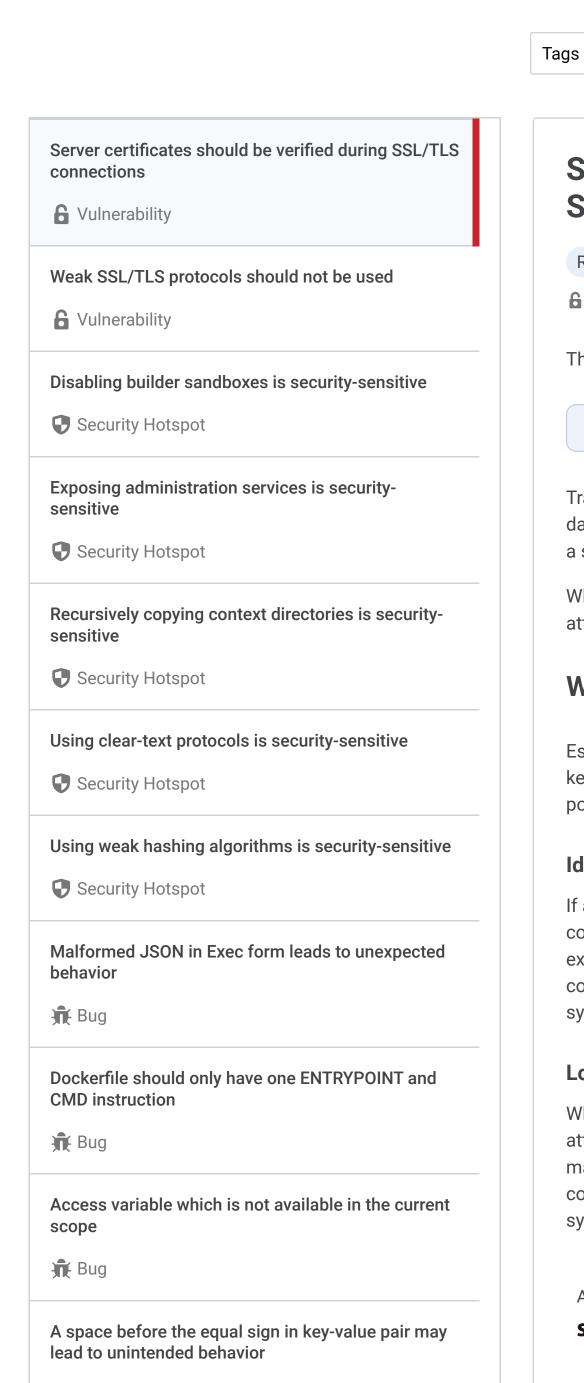
VB.NET



Docker static code analysis

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

Code Smell (21) *Bug 4 Security Hotspot (15) All rules 44 **6** Vulnerability (4)



Bug

Server certificates should be verified during **SSL/TLS connections**

Analyze your code

Search by name..

Responsibility - Trustworthy Security (2) cwe privacy ssl

Impact

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

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

Transport Layer Security (TLS) provides secure communication between systems over the internet by encrypting the data sent between them. Certificate validation adds an extra layer of trust and security to this process to ensure that a system is indeed the one it claims to be.

Clean code attribute

When certificate validation is disabled, the client skips a critical security check. This creates an opportunity for attackers to pose as a trusted entity and intercept, manipulate, or steal the data being transmitted.

What is the potential impact?

Establishing trust in a secure way is a non-trivial task. When you disable certificate validation, you are removing a key mechanism designed to build this trust in internet communication, opening your system up to a number of potential threats.

Identity spoofing

If a system does not validate certificates, it cannot confirm the identity of the other party involved in the communication. An attacker can exploit this by creating a fake server and masquerading as a legitimate one. For example, they might set up a server that looks like your bank's server, tricking your system into thinking it is communicating with the bank. This scenario, called identity spoofing, allows the attacker to collect any data your system sends to them, potentially leading to significant data breaches.

Loss of data integrity

When TLS certificate validation is disabled, the integrity of the data you send and receive cannot be guaranteed. An attacker could modify the data in transit, and you would have no way of knowing. This could range from subtle manipulations of the data you receive to the injection of malicious code or malware into your system. The consequences of such breaches of data integrity can be severe, depending on the nature of the data and the system.

Available In: sonarlint ⊕ | sonarcloud 🔂 | sonarqube

© 2008-2024 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE, SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All r expressly reserved.

