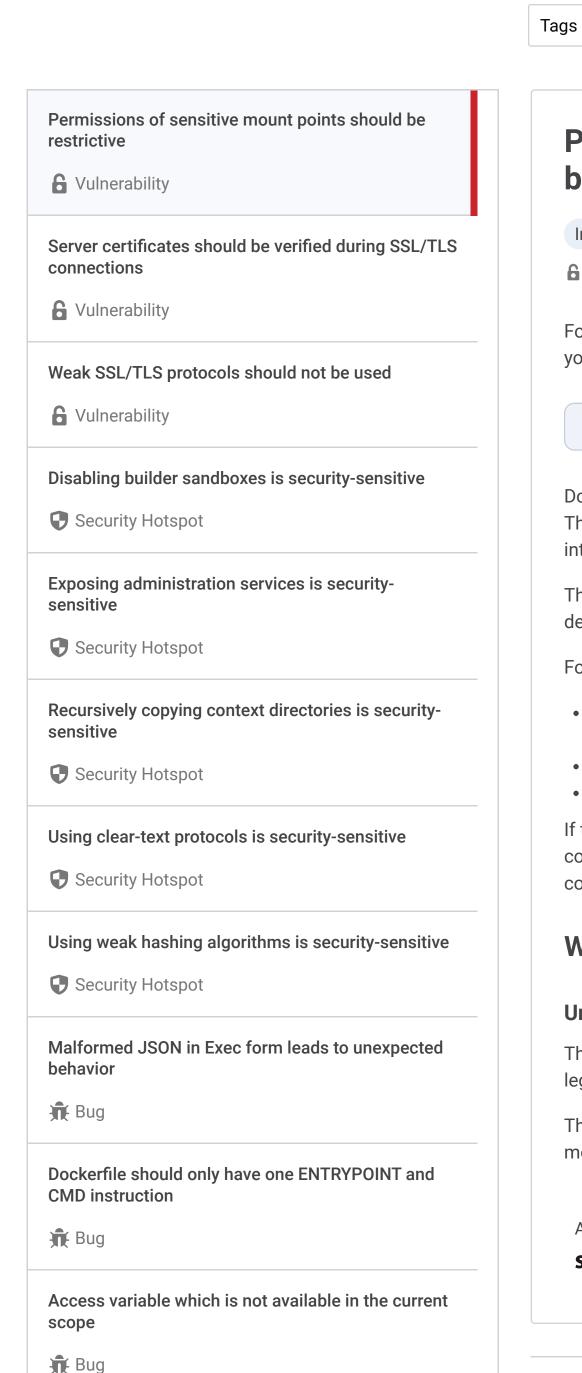




Docker static code analysis

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





Analyze your code

Search by name..

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

Impact

Docker offers a feature to mount files and directories for specific RUN instructions when building Docker images. This feature can be used to provide secrets to commands that are executed during the build without baking them into the image. Additionally, it can be used to access SSH agents during the build.

you set this mode so that any user of the operating system can access the mount, it is vulnerable to leaks.

Clean code attribute

The mode option is an octal value that allows you to specify the permissions for a particular file or directory. By default, on Docker, when mounting a secret, it is set to 0400.

For ssh, it is set by default to 0600:

Intentionality - Complete Security (2)

- The first digit 0 stands for special permissions (like setuid, setgid and sticky bit) and in this case means that no special permissions are set.
- The following 6 (4+2 in octal format) means that the owner has read (4) and write (2) permissions
- 00 means that the group and others have no permissions.

If the others bit is set to a value other than 0 at build-time, any other process can access it when the RUN command is executed: the secrets are vulnerable to supply chain attacks that aim to siphon secrets from containers.

What is the potential impact?

Unauthorized access

The unintended audience can exploit the leaked private key or equivalent to authenticate themselves as the legitimate owner, gaining unauthorized entry to systems, servers, or accounts that accept the key for authentication.

This unauthorized access opens the door for various malicious activities, including data breaches, unauthorized modifications, and misuse of sensitive information.

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 riexpressly reserved.

