Enforcing Container Security with Anchore

Riley Wood

riley.wood@utexas.edu

What is Anchore?

- Continuous integration testing for containers

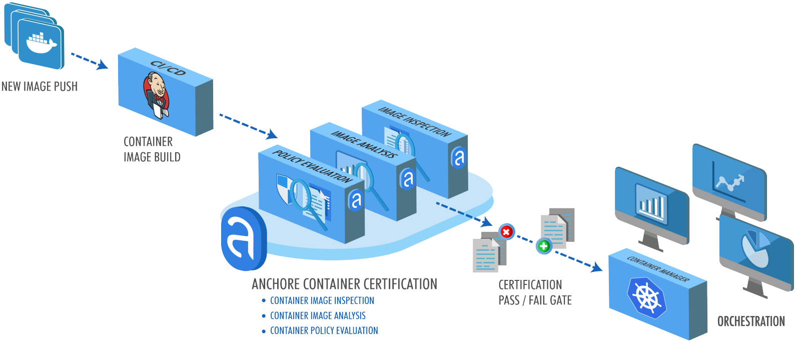
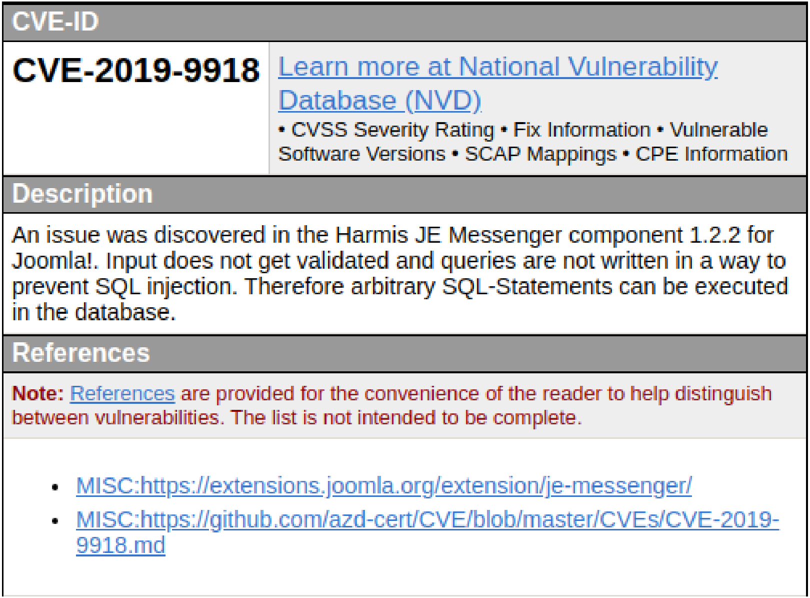


Figure 1: Anchore Diagram

Anchore Features

- Easily test for known vulnerabilities (CVEs)
  - https://www.cvedetails.com/
- Define your own security policies
- Integrates with Kubernetes
  - https://anchore.com/kubernetes/

Example CVE



CVE-ID

CVE-2019-9918

Learn more at National Vulnerability Database (NVD)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

An issue was discovered in the Harmis JE Messenger component 1.2.2 for Joomla!. Input does not get validated and queries are not written in a way to prevent SQL injection. Therefore arbitrary SQL-Statements can be executed in the database.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://extensions.joomla.org/extension/je-messenger/
- MISC:https://github.com/azd-cert/CVE/blob/master/CVEs/CVE-2019-9918.md

Figure 2: CVE-2019-9918

Containers' Implications for Security

- Devs can constrain containers to only that SW which is needed to run their app
    - Reduces the chance of a vulnerability arising since there is less software to exploit
- Anchore can also be used to make sure certain known-vulnerable libraries are excluded from your container
    - Helps to ensure that the minimum set of software is also secure

Security with Anchore

- Container ensures available software is minimized
- Anchore ensures that software is audited for known vulnerabilities.

Demo

- Anchore integration with Docker compose
- https://hub.docker.com/r/anchore/anchore-engine

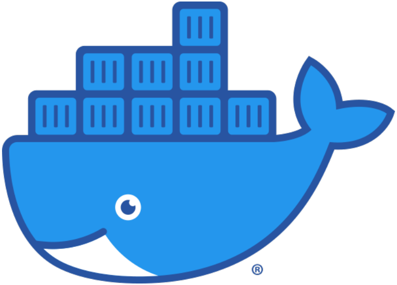


Figure 3: Docker logo

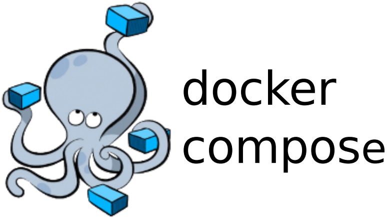


Figure 4: Docker compose