Vulnerability & Misconfiguration Scanner - Trivy



Agenda

- What did you do for your artifacts to ensure its security & configuration correct?
- What kind of concern are?
- Trivy An vulnerability & misconfiguration scanner tool
- Difficult to use?
- Q&A

What did you do for your artifacts to ensure its security & configuration correct?

Docker Image

• Push image to registry directly

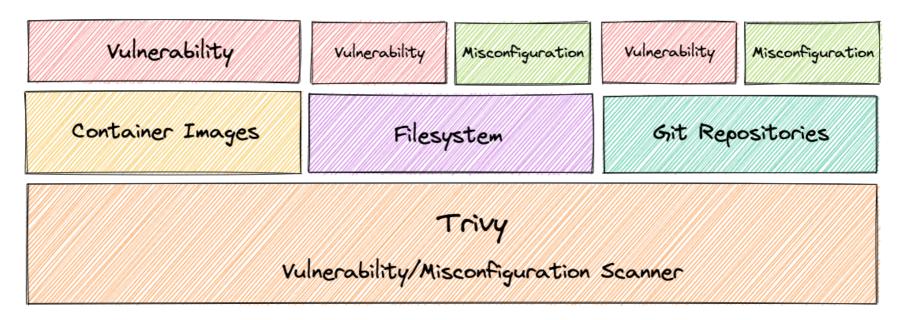
What kind of concern are?

Maybe

- Your base image has know/unfixed vulnerabilities
- Your artifacts contains some wrong config
- Your write some backdoor unconsciously
- ...

Trivy - An vulnerability & misconfiguration scanner tool

Capability



Working principle







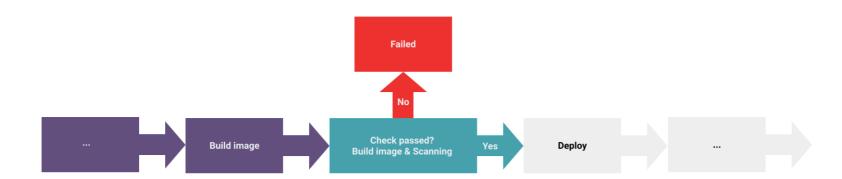


1

Difficult to use?

Talks is cheep, show me code

Pipeline



Image

```
docker run --rm -v \
  /var/run/docker.sock:/var/run/docker.sock \
  aquasec/trivy image \
  --severity HIGH, CRITICAL \
  --exit-code 1 \
  dashboard:${{ github.sha }}
```

https://github.com/guzhongren/Buildkite-

Dashboard/runs/4087037441?

```
Trivy scanner
   ▼ Run docker run --rm -v /var/run/docker.sock:/var/run/docker.sock
     docker run --rm -v /var/run/docker.sock:/var/run/docker.sock
        aguasec/trivy image --severity HIGH, CRITICAL --exit-code 1
    dashboard:dc266d0260f05098138d5b03797cebdfe72b7842
     shell: /usr/bin/bash -e {0}
   Unable to find image 'aquasec/trivy:latest' locally
   latest: Pulling from aquasec/trivy
   a0d0a0d46f8b: Already exists
8 bff5b5a771f2: Pulling fs laver
   818276ee1efb: Pulling fs layer
10 c83f610988b2: Pulling fs layer
   c83f610988b2: Verifying Checksum
   c83f610988b2: Download complete
   818276eelefb: Verifying Checksum
   818276ee1efb: Download complete
15 bff5b5a771f2: Verifying Checksum
   bff5b5a771f2: Download complete
   bff5b5a771f2: Pull complete
   818276ee1efb: Pull complete
   c83f610988b2: Pull complete
   Digest: sha256:14afd8ec72df184bc5e2b0d0891865ce5037c14d41d4af571cd0a78fe3981e03
   Status: Downloaded newer image for aquasec/trivy:latest
   2021-11-03T00:21:02.723Z
                                       Need to update DB
   2021-11-03T00:21:02.723Z
                                       Downloading DB...
   2021-11-03T00:21:07.346Z
                                       Detected OS: debian
    2021-11-03T00:21:07.346Z
                                      Detecting Debian vulnerabilities...
   2021-11-03T00:21:07.367Z
                                      Number of language-specific files: 0
   dashboard:dc266d0260f05098138d5b03797cebdfe72b7842 (debian 10.11)
   Total: 30 (HIGH: 26, CRITICAL: 4)
       LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
   TITLE
                   | CVE-2021-22946 | HIGH
                                                | 7.64.0-4+deb10u2
                                                                                        | curl: Requirement to use
                                                                                        I TLS not properly
```

Repo

```
docker run --rm -v \
  /var/run/docker.sock:/var/run/docker.sock \
  aquasec/trivy repo \
  --severity HIGH, CRITICAL \
  --exit-code 1 \
  https://github.com/guzhongren/Buildkite-Dashboard
```

https://github.com/guzhongren/Buildkite-

Dashboard/runs/4093499534?

```
    Scan repo

     ▼ Run docker run --rm -v \
        docker run --rm -v \
            /var/run/docker.sock:/var/run/docker.sock \
            aquasec/trivy repo \
           --severity HIGH, CRITICAL \
           guzhongren/Buildkite-Dashboard
        shell: /usr/bin/bash -e {0}
      2021-11-02T15:01:41.503Z INFO
      2021-11-02T15:01:41.503Z INFO
     Enumerating objects: 141, done.
     Counting objects: 0% (1/141)
      Counting objects: 1% (2/141)
      Counting objects: 2% (3/141)
      Counting objects: 3% (5/141)
  15 Counting objects: 4% (6/141)
      Counting objects: 5% (8/141)
```

```
Scan repo
220 package-lock.json (npm)
222 Total: 1 (HIGH: 1, CRITICAL: 0)
225 | LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
                                                                                            TITLE
                                                            | 4.17.21
227 | lodash | CVE-2021-23337 | HIGH | 4.17.19
                                                                           | nodejs-lodash: command
                                                                           | injection via template
                                                                           | -->avd.aquasec.com/nvd/cve-2021-
232 yarn.lock (yarn)
234 Total: 2 (HIGH: 2, CRITICAL: 0)
      LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
239 | ansi-regex | CVE-2021-3807 | HIGH
                                                       | 5.0.1, 6.0.1 | nodejs-ansi-regex: Regular
                                                                              | expression denial of service
```

FS

```
docker run --rm -v \
  /var/run/docker.sock:/var/run/docker.sock \
  aquasec/trivy fs \
  --severity HIGH, CRITICAL \
  --exit-code 1 \
  ./
```

• https://github.com/guzhongren/Buildkite-

Dashboard/runs/4093499534?

```
docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
   aguasec/trivv fs \
    --- severity HIGH, CRITICAL \
latest: Pulling from aguasec/trivy
a8d@a@d46f8b: Already exists
Digest: sha256:14afd8ec72df184bc5e2b8d8891865ce5037c14d41d4af571cd8a78fe3981e03
Status: Downloaded newer image for aquasec/trivy:latest
2821-11-02T15:01:39.686Z INFO Detecting Alpine vulnerabilities..
2021-11-02T15:01:39.688Z INFO Number of language-specific files: 0
d929756d09e8 (alpine 3.14.2)
                                                                            ] 9.78% ? p/s ?5.63 MiB / 24.53 MiB [--
                                                                                                                                                                    1 22.96% ?
                                                                                                                                                            __] 52.04% 17.31 MiB
p/s 78.88 MiB / 24.53 MiB [--
                                                                               __] 36.21% ? p/s ?12.77 MiB / 24.53 MiB [---
MIB p/s ETA 0s24.53 MIB / 24.53 MIB [
```

Config

```
docker run --rm -v \
  /var/run/docker.sock:/var/run/docker.sock \
  aquasec/trivy config \
  --severity HIGH, CRITICAL \
  --security-checks vuln, config \
  --exit-code 1 \
  ./
```

https://github.com/guzhongren/Buildkite-

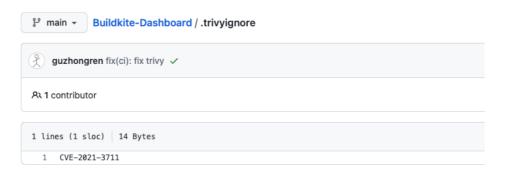
Dashboard/runs/4093499534?

.trivyignore

CVE-2021-3711

https://github.com/guzhongren/Buildkite-

Dashboard/blob/main/.trivyignore



Refs

- https://aquasecurity.github.io/trivy
- https://github.com/aquasecurity/trivy
- http://guzhongren.github.io/2021/08/container-image-scanner-trivy/
- ...

Q&A

Thank you!