

Vulnerability & Misconfiguration Scanner - Trivy



aqua
trivy

@guzhongren 2021-10

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

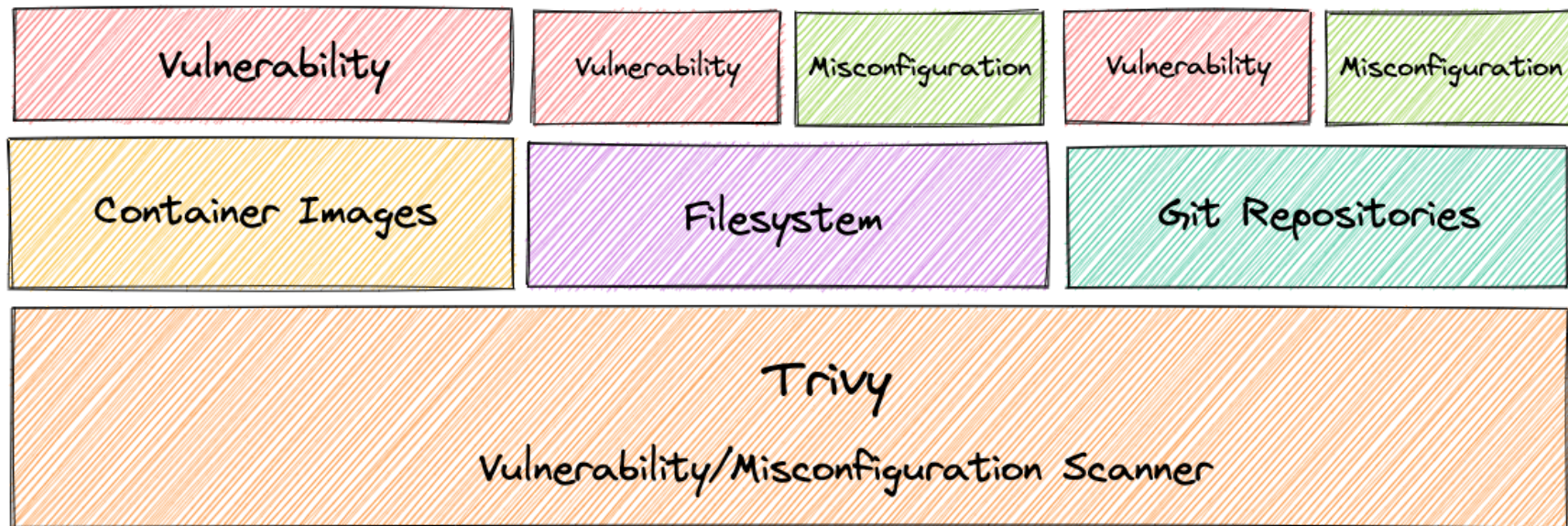
What kind of concern are?

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

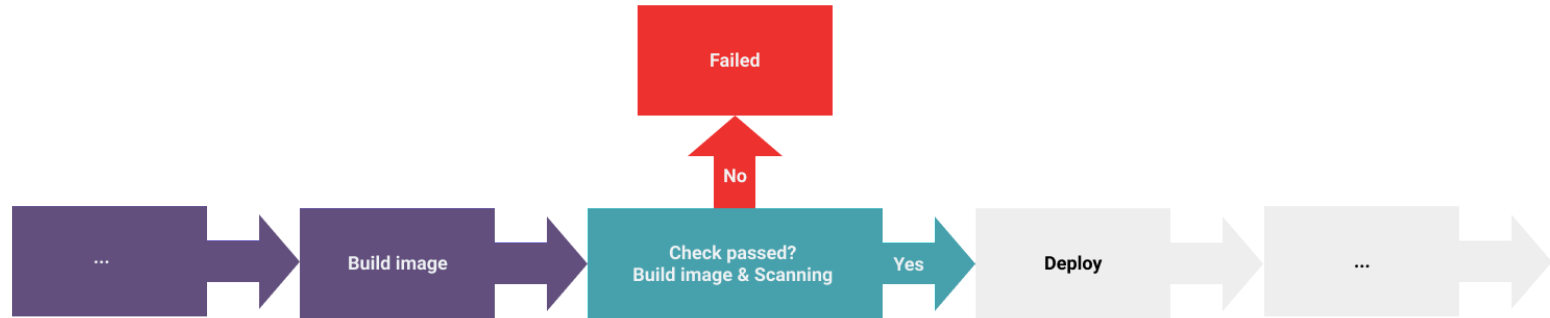


2

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.ref }}
```

- <https://github.com/aquasecurity/trivy>
- Dashboard/runs/4
- check_suite_focus

```
Trivy scanner
1 Run docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
2 docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
3 aquasec/trivy image --severity HIGH,CRITICAL --exit-code 1
4 dashboard:dc266d8268f8589813d5d83797cebdfe72b7842
5 shell: /usr/bin/bash -e (0)
6 Unable to find image 'aquasec/trivy:latest' locally
7 latest: Pulling from aquasec/trivy
8 a0d8a0d46f8b: Already exists
9 bff55a771f2: Pulling fs layer
10 818276ee1fb: Pulling fs layer
11 c83f618988b2: Pulling fs layer
12 c83f618988b2: Verifying Checksum
13 c83f618988b2: Download complete
14 818276ee1fb: Verifying Checksum
15 818276ee1fb: Download complete
16 bff55a771f2: Verifying Checksum
17 bff55a771f2: Download complete
18 bff55a771f2: Pull complete
19 818276ee1fb: Pull complete
20 c83f618988b2: Pull complete
21 Digest: sha256:14f0bec72d1f84bc5e2b08081865ce5831c14d41d4af571cd8a78fe3981e83
22 Status: Downloaded newer image for aquasec/trivy:latest
23 2021-11-03T00:21:02.723Z INFO Need to update DB
24 2021-11-03T00:21:02.723Z INFO Downloading DB...
25 2021-11-03T00:21:07.346Z INFO Detected OS: debian
26 2021-11-03T00:21:07.346Z INFO Detecting Debian vulnerabilities...
27 2021-11-03T00:21:07.307Z INFO Number of language-specific files: 0
28 dashboard:dc266d8268f8589813d5d83797cebdfe72b7842 (debian 10.11)
29 =====
30 Total: 30 (HIGH: 26, CRITICAL: 4)
31
32
33 | LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
34 | TITLE |
35 | curl | CVE-2021-22946 | HIGH | 7.64.0-4+deb10u2 | | curl: Requirement to use
36 | | | | | | | | TLS not properly
   enforced |
```

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/g
```

- <https://github.com/aquasecurity/trivy>
Dashboard/runs/4
check_suite_focus

Scan repo

219 package-lock.json (npm)
220 =====
221 Total: 1 (HIGH: 1, CRITICAL: 0)
222
223
224

LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE
lodash	CVE-2021-23337	HIGH	4.17.19	4.17.21	nodejs-lodash: command injection via template

225
226
227
228
229
230
231

231 yarn.lock (yarn)
232 =====
233 Total: 2 (HIGH: 2, CRITICAL: 0)
234
235
236

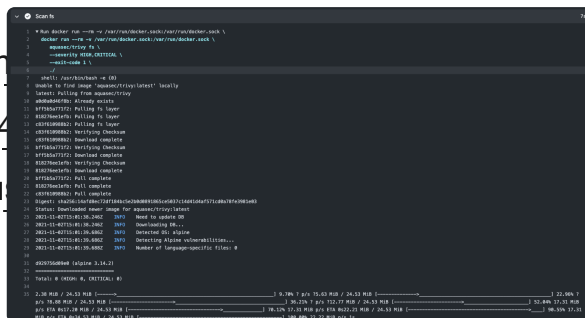
LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE
ansi-regex	CVE-2021-3887	HIGH	3.0.0	5.0.1, 6.0.1	nodejs-ansi-regex: Regular expression denial of service (ReDoS) matching ANSI escape codes

237
238
239
240
241
242
243
244

FS

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

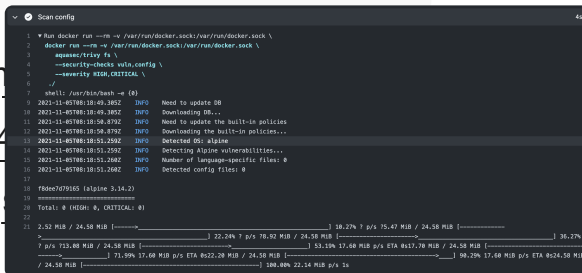
- https://github.com/GoogleCloudPlatform/terraform-google-compute/blob/master/.github/workflows/check_suite_focus.yml



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/aquasecurity/trivy>
Dashboard/runs/4
check_suite_focus

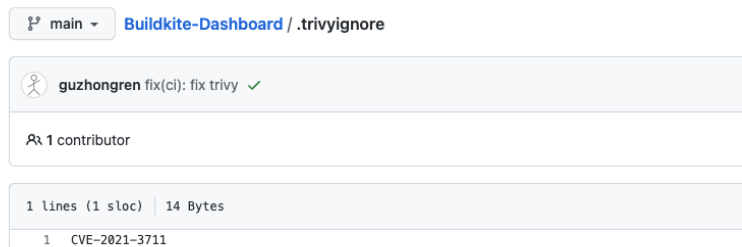


```
Scan config
1 Run docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
2 docker run --rm -v /var/run/docker.sock:/var/run/docker.sock \
3 aquasec/trivy fa \
4 --security-checks vuln,config \
5 --severity HIGH,CRITICAL \
6 ./
7 shell: /usr/bin/bash -e
8 2021-11-05T00:10:40.280Z INFO Need to update DB
9 2021-11-05T00:10:40.380Z INFO Downloading DB...
10 2021-11-05T00:10:50.470Z INFO Need to update the built-in policies
11 2021-11-05T00:10:50.470Z INFO Downloading the built-in policies...
12 2021-11-05T00:10:51.200Z INFO Detected CVE: alpine
13 2021-11-05T00:10:51.200Z INFO Detecting Alpine vulnerabilities...
14 2021-11-05T00:10:51.200Z INFO Number of language-specific files: 0
15 2021-11-05T00:10:51.200Z INFO Detected config files: 0
16
17 f8dee079505 (alpine 3.14.2)
18 =====
19 Total: 0 (HIGH: 0, CRITICAL: 0)
20
21 2.52 MiB / 24.58 MiB [-----] 10.27% 7 p/s 75.47 MiB / 24.58 MiB [-----] 36.27%
22 7 p/s 73.48 MiB / 24.58 MiB [-----] 30.12% 17.68 MiB p/s ETA 0:17.78 MiB / 24.58 MiB [-----] 71.99% 17.68 MiB p/s ETA 0:22.28 MiB / 24.58 MiB [-----] 98.29% 17.68 MiB p/s ETA 0:24.58 MiB
23 / 24.58 MiB [-----] 200.00% 22.14 MiB p/s 1s
```

.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!