Vulnerability & Misconfiguration Scanner - Trivy

@guzhongren 2021-10

Agenda

- What did you do for your artifacts to ensure its security & configuration correct?
- What kind of concern are?
- Trivy - a vulnerability & misconfiguration scanner tool
- Difficult to use? Talks is cheep, show me code.
- Practice in our project
- Q&A

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

Docker Image

- Push image to registry directly

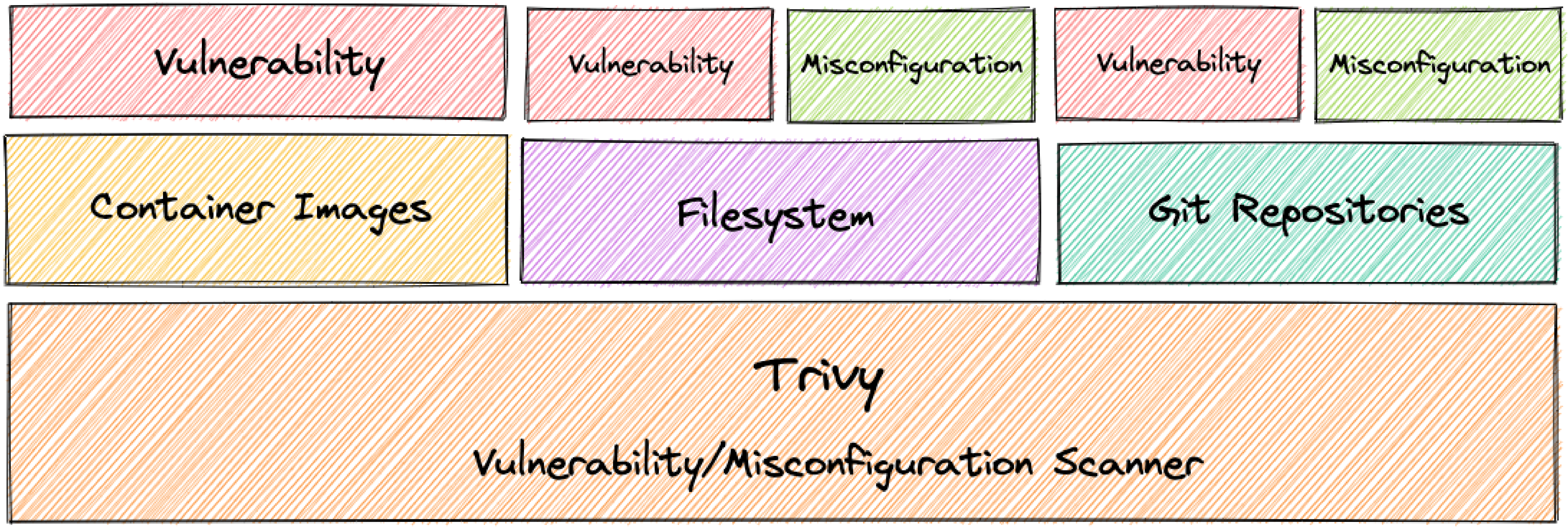
What kind of concern are?

Maybe

- Your base image has know/unfixed vulnerabilities
- Your image contains some secret config
- Your write some backdoor unconsciously
- …

Trivy - a vulnerability & misconfiguration scanner tool

Capability



Vulnerability

Vulnerability

Misconfiguration

Vulnerability

Misconfiguration

Container Images

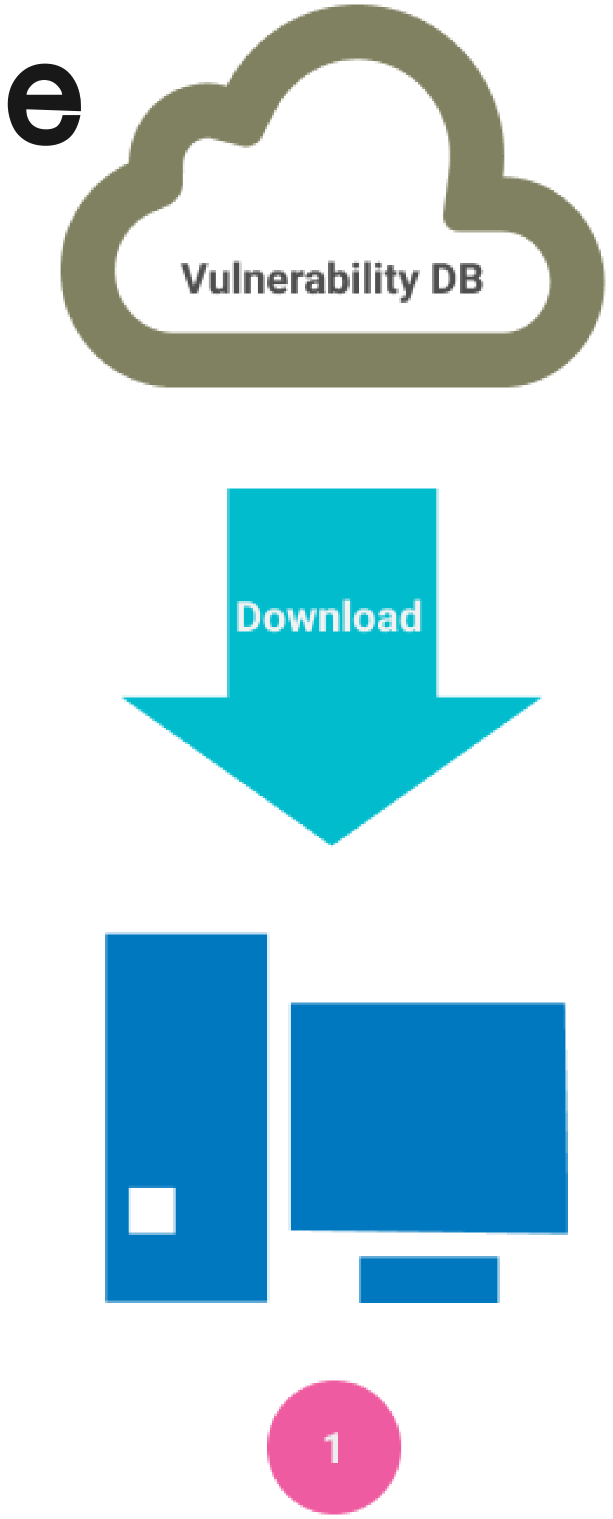
Filesystem

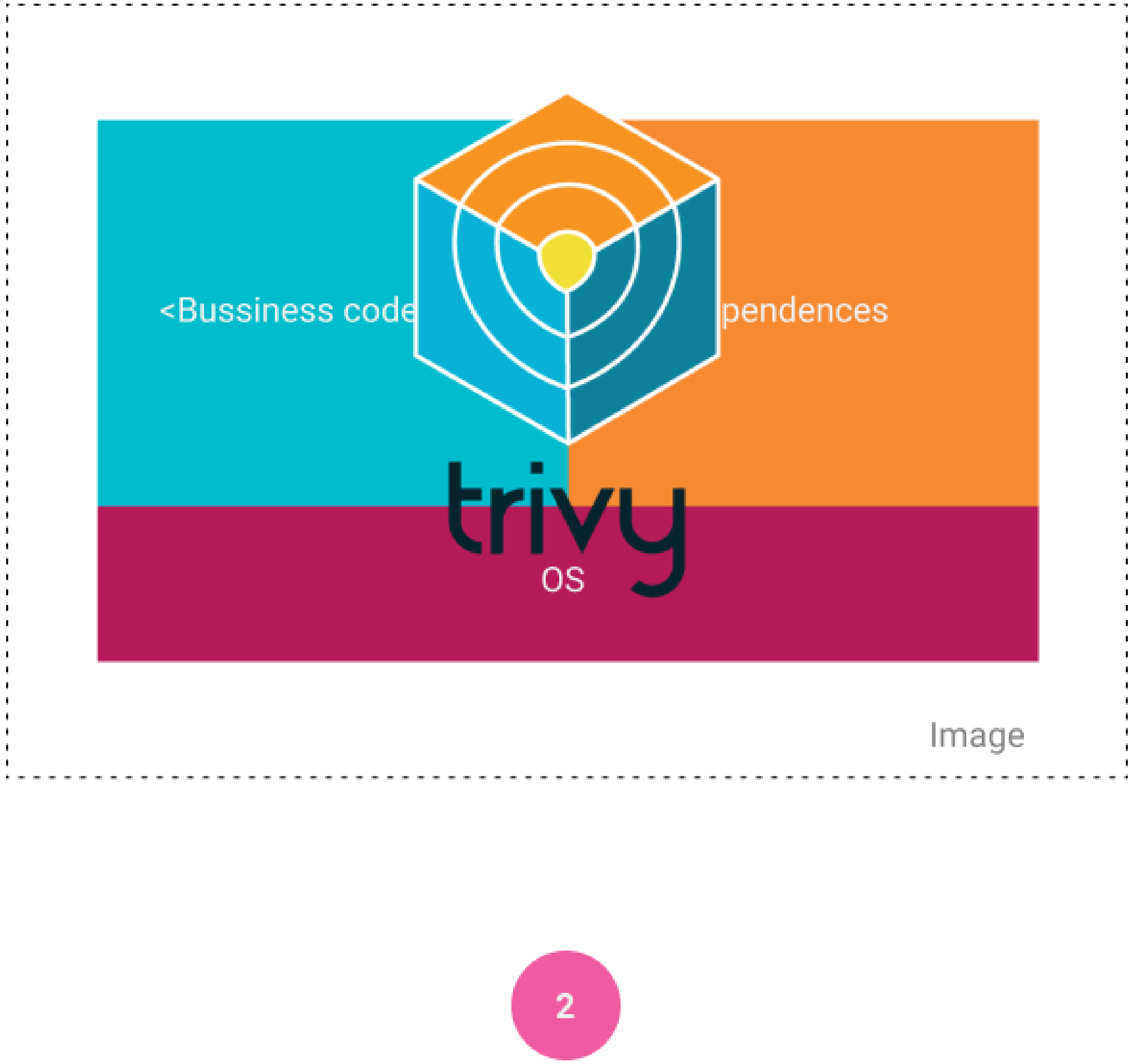
Git Repositories

Trivy

Vulnerability/Misconfiguration Scanner

Working principle

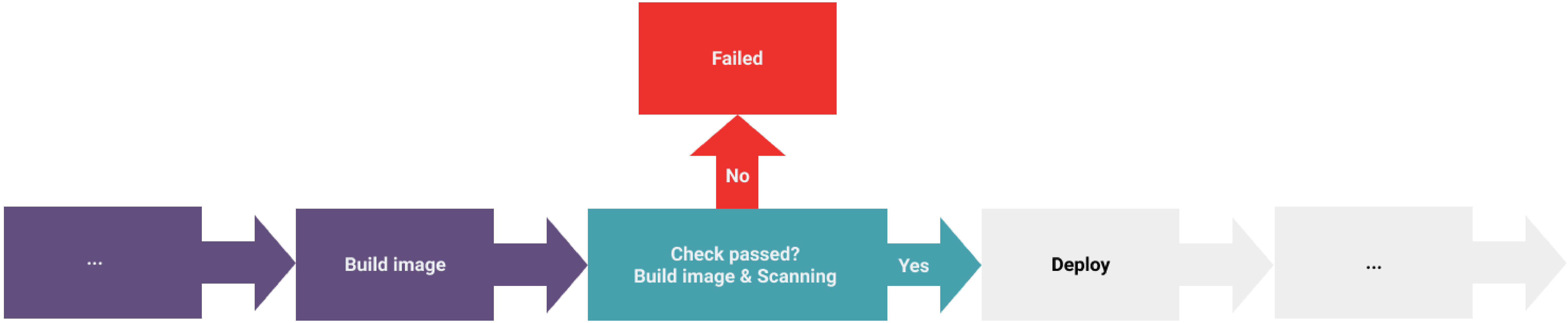




Difficult to use?

Talks is cheep, show me code.

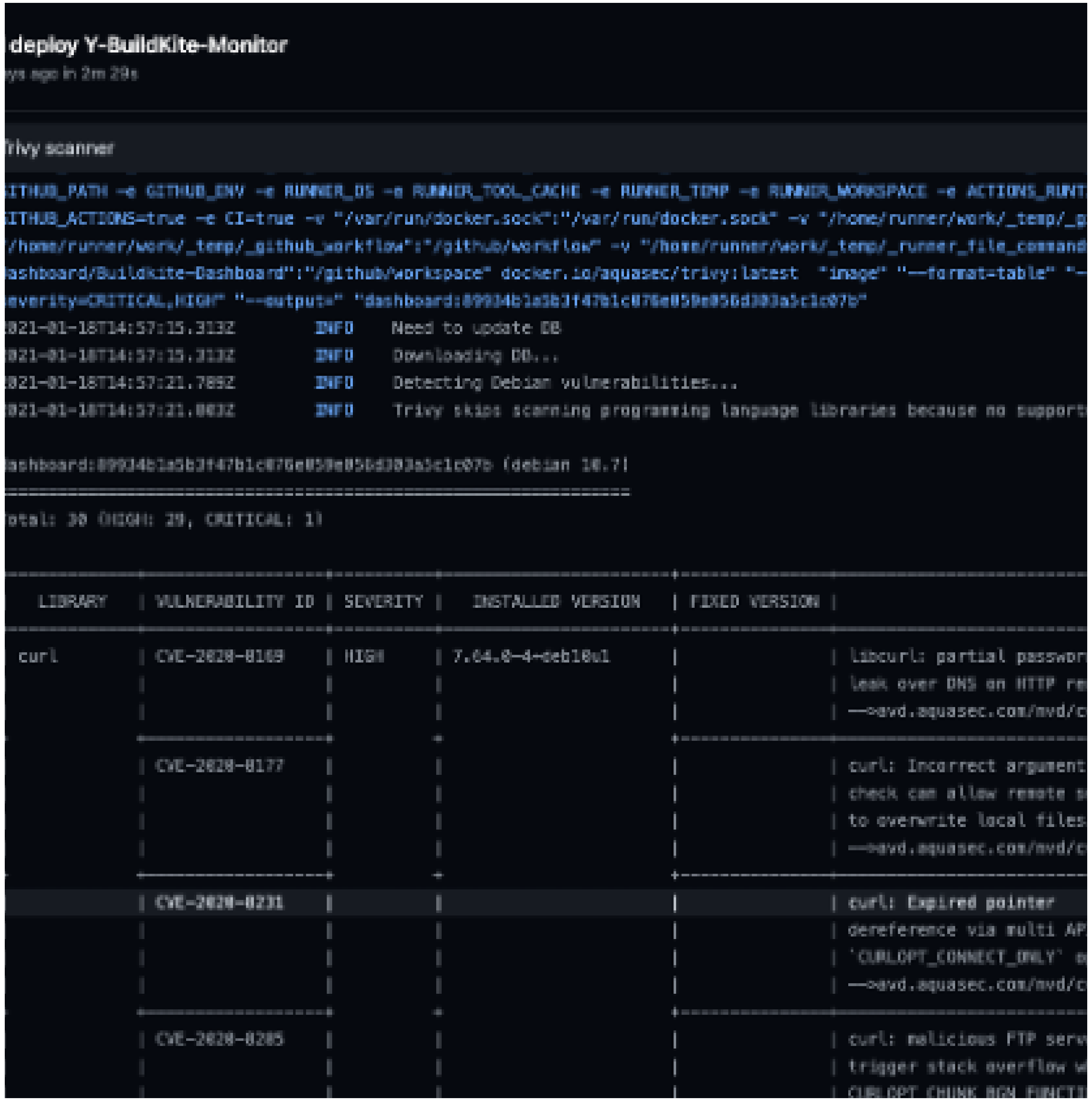
Pipeline


Failed
No
...
Build image
Check passed?
Build image & Scanning
Yes
Deploy
...

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/4080949199?check_suite_focus=true



deploy Y-BuildKite-Monitor

ys ago in 2m 29s

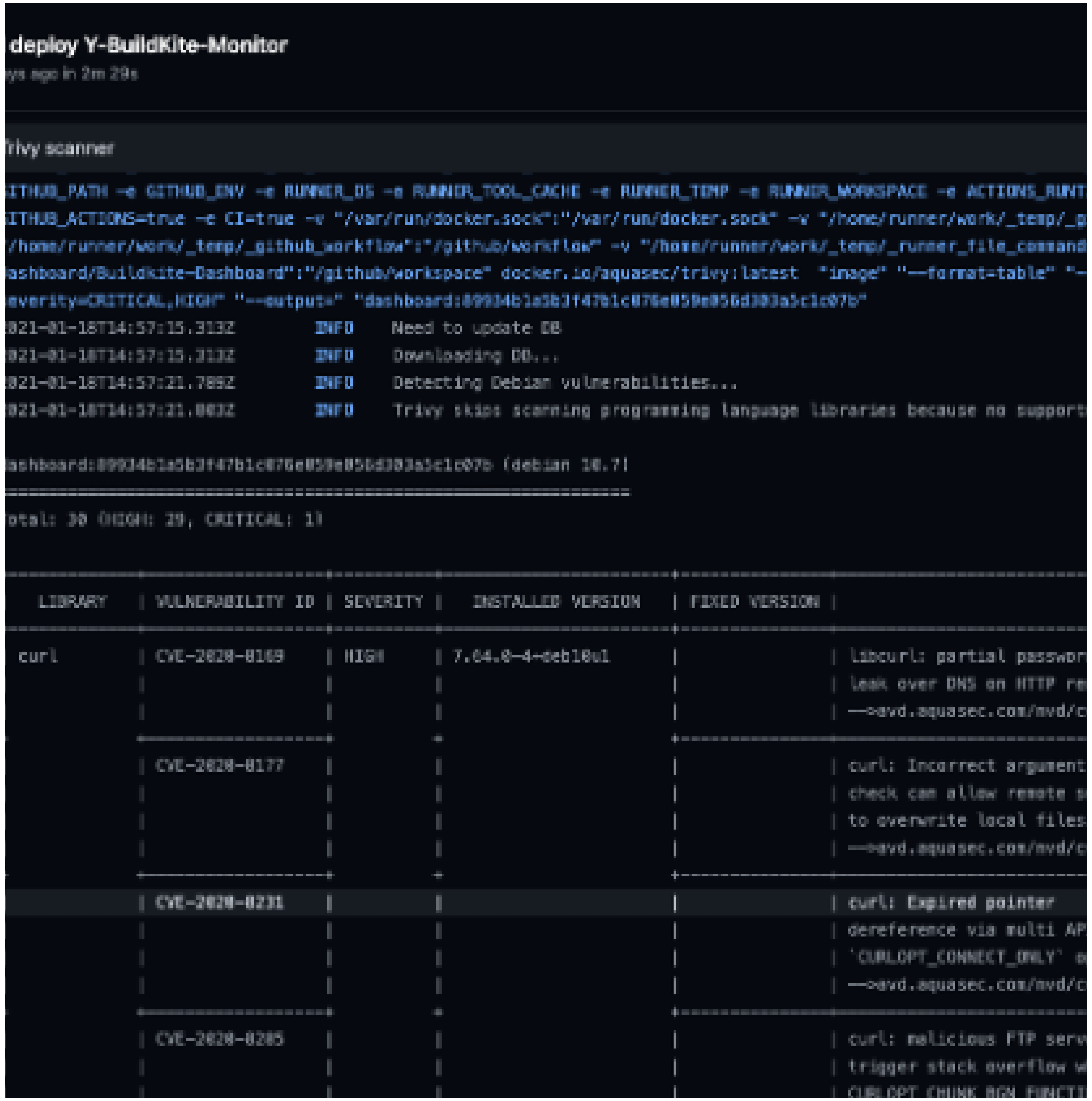
rivy scanner

```
ITHUB_PATH -e GITHUB_ENV -e RUNNER_OS -e RUNNER_TOOL_CACHE -e RUNNER_TEMP -e RUNNER_WORKSPACE -e ACTIONS_RUNT
ITHUB_ACTIONS=true -e CI=true -v "/var/run/docker.sock":"/var/run/docker.sock" -v "/home/runner/work/_temp/_g
/home/runner/work/_temp/_github_workflow":"/github/workflow" -v "/home/runner/work/_temp/_runner_file_command
ashboard/Buildkite-Dashboard":"/github/workspace" docker.io/aquasec/trivy:latest  "image" "--format=table" "-
everity=CRITICAL,HIGH" "--output=" "dashboard:89934b1a5b3f47b1c876e859e856d303a5c1c07b"
021-01-18T14:57:15.313Z        INFO    Need to update DB
021-01-18T14:57:15.313Z        INFO    Downloading DB...
021-01-18T14:57:21.789Z        INFO    Detecting Debian vulnerabilities...
021-01-18T14:57:21.803Z        INFO    Trivy skips scanning programming language libraries because no support

ashboard:89934b1a5b3f47b1c876e859e856d303a5c1c07b (debian 10.7)
=================================================================
otal: 30 (HIGH: 29, CRITICAL: 1)

+--------------+------------------+----------+-------------------+---------------+--------------------
   LIBRARY     | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
+--------------+------------------+----------+-------------------+---------------+--------------------
 curl          | CVE-2020-8169    | HIGH     | 7.64.0-4+deb10u1  |               | libcurl: partial passwor
               |                  |          |                   |               | leak over DNS on HTTP re
               |                  |          |                   |               | -->avd.aquasec.com/nvd/c
               +------------------+          +                   +---------------+--------------------
               | CVE-2020-8177    |          |                   |               | curl: Incorrect argument
               |                  |          |                   |               | check can allow remote s
               |                  |          |                   |               | to overwrite local files
               |                  |          |                   |               | -->avd.aquasec.com/nvd/c
               +------------------+          +                   +---------------+--------------------
               | CVE-2020-8231    |          |                   |               | curl: Expired pointer
               |                  |          |                   |               | dereference via multi AP
               |                  |          |                   |               | `CURLOPT_CONNECT_ONLY` o
               |                  |          |                   |               | -->avd.aquasec.com/nvd/c
               +------------------+          +                   +---------------+--------------------
               | CVE-2020-8285    |          |                   |               | curl: malicious FTP serv
               |                  |          |                   |               | trigger stack overflow w
               |                  |          |                   |               | CURLOPT_CHUNK_BGN_FUNCTI
```

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/4081563022?check_suite_focus=true



deploy Y-BuildKite-Monitor

ys ago in 2m 29s

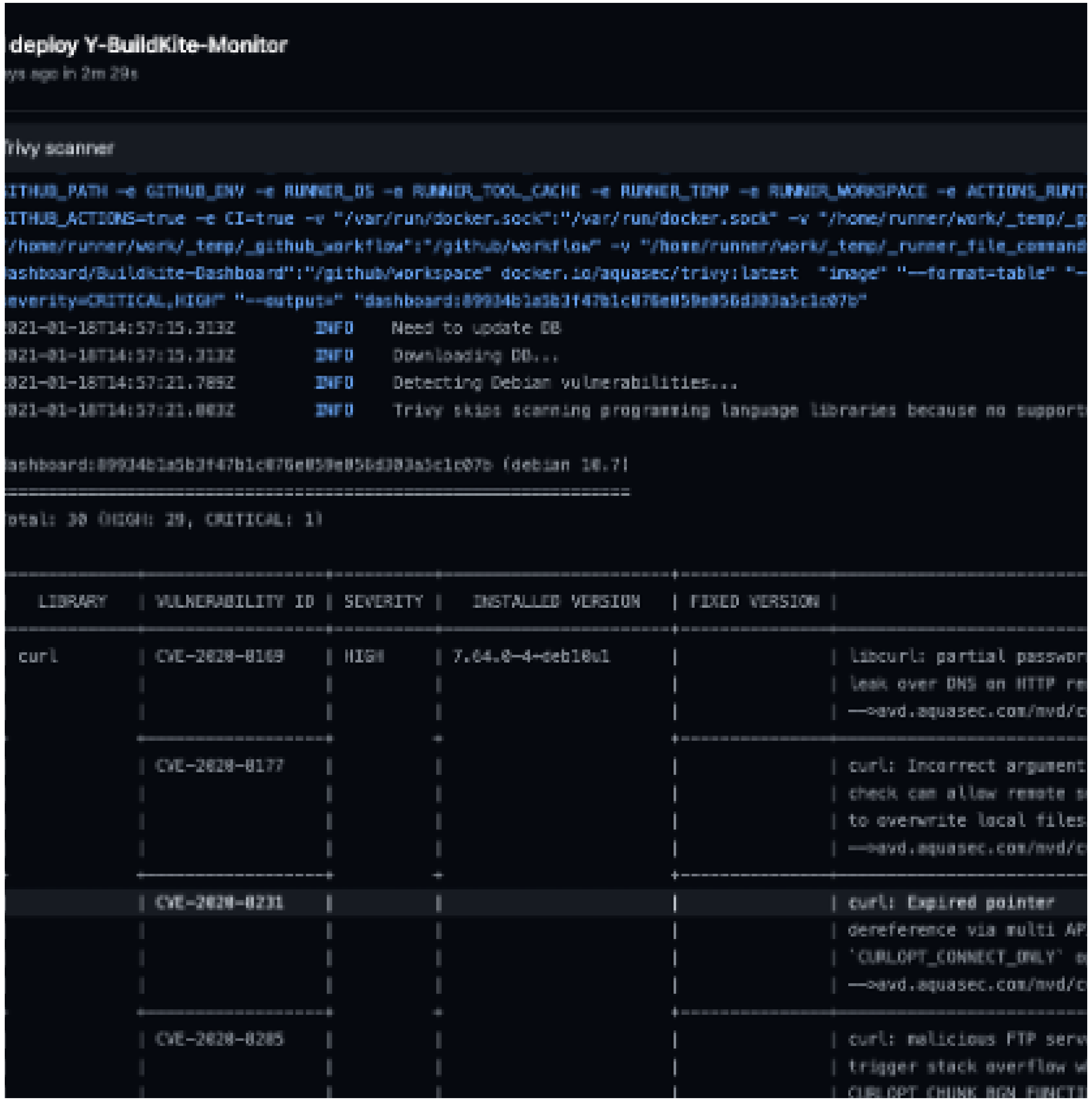
rivy scanner

```
ITHUB_PATH -e GITHUB_ENV -e RUNNER_OS -e RUNNER_TOOL_CACHE -e RUNNER_TEMP -e RUNNER_WORKSPACE -e ACTIONS_RUNT
ITHUB_ACTIONS=true -e CI=true -v "/var/run/docker.sock":"/var/run/docker.sock" -v "/home/runner/work/_temp/_g
/home/runner/work/_temp/_github_workflow":"/github/workflow" -v "/home/runner/work/_temp/_runner_file_command
ashboard/Buildkite-Dashboard":"/github/workspace" docker.io/aquasec/trivy:latest  "image" "--format=table" "-
everity=CRITICAL,HIGH" "--output=" "dashboard:89934b1a5b3f47b1c876e059e056d303a5c1c07b"
021-01-18T14:57:15.313Z        INFO    Need to update DB
021-01-18T14:57:15.313Z        INFO    Downloading DB...
021-01-18T14:57:21.789Z        INFO    Detecting Debian vulnerabilities...
021-01-18T14:57:21.803Z        INFO    Trivy skips scanning programming language libraries because no support

ashboard:89934b1a5b3f47b1c876e059e056d303a5c1c07b (debian 10.7)
==================================================================

otal: 30 (HIGH: 29, CRITICAL: 1)

-------------+------------------+----------+-------------------+---------------+-----------------------
  LIBRARY    | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
-------------+------------------+----------+-------------------+---------------+-----------------------
 curl        | CVE-2020-8169    | HIGH     | 7.64.0-4+deb10u1  |               | libcurl: partial passwor
             |                  |          |                   |               | leak over DNS on HTTP re
             |                  |          |                   |               | -->avd.aquasec.com/nvd/c
             +------------------+          +                   +---------------+-----------------------
             | CVE-2020-8177    |          |                   |               | curl: Incorrect argument
             |                  |          |                   |               | check can allow remote s
             |                  |          |                   |               | to overwrite local files
             |                  |          |                   |               | -->avd.aquasec.com/nvd/c
             +------------------+          +                   +---------------+-----------------------
             | CVE-2020-8231    |          |                   |               | curl: Expired pointer
             |                  |          |                   |               | dereference via multi AP
             |                  |          |                   |               | `CURLOPT_CONNECT_ONLY` o
             |                  |          |                   |               | -->avd.aquasec.com/nvd/c
             +------------------+          +                   +---------------+-----------------------
             | CVE-2020-8285    |          |                   |               | curl: malicious FTP serv
             |                  |          |                   |               | trigger stack overflow w
             |                  |          |                   |               | CURLOPT_CHUNK_BGN_FUNCTI
```

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/4081563022?check_suite_focus=true



deploy Y-BuildKite-Monitor

ys ago in 2m 29s

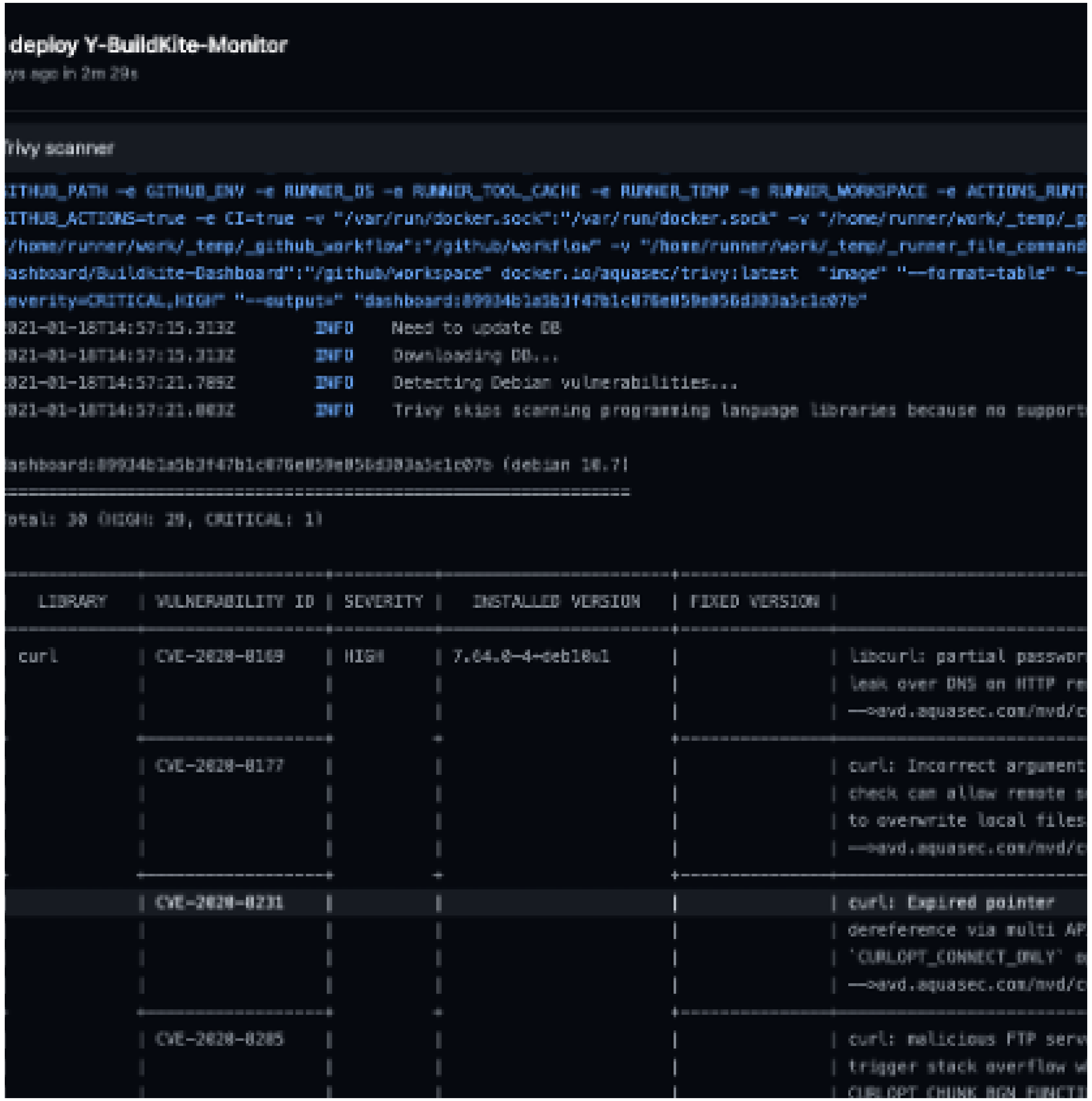
rivy scanner

```
ITHUB_PATH -e GITHUB_ENV -e RUNNER_OS -e RUNNER_TOOL_CACHE -e RUNNER_TEMP -e RUNNER_WORKSPACE -e ACTIONS_RUNT
ITHUB_ACTIONS=true -e CI=true -v "/var/run/docker.sock":"/var/run/docker.sock" -v "/home/runner/work/_temp/_g
/home/runner/work/_temp/_github_workflow":"/github/workflow" -v "/home/runner/work/_temp/_runner_file_command
ashboard/Buildkite-Dashboard":"/github/workspace" docker.io/aquasec/trivy:latest  "image" "--format=table" "--
everity=CRITICAL,HIGH" "--output=" "dashboard:89934b1a5b3f47b1c876e859e856d303a5c1c07b"
021-01-18T14:57:15.313Z        INFO    Need to update DB
021-01-18T14:57:15.313Z        INFO    Downloading DB...
021-01-18T14:57:21.789Z        INFO    Detecting Debian vulnerabilities...
021-01-18T14:57:21.803Z        INFO    Trivy skips scanning programming language libraries because no support

ashboard:89934b1a5b3f47b1c876e859e856d303a5c1c07b (debian 10.7)
=================================================================
otal: 30 (HIGH: 29, CRITICAL: 1)

-----------+------------------+----------+-------------------+---------------+-------------------
  LIBRARY  | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
-----------+------------------+----------+-------------------+---------------+-------------------
 curl      | CVE-2020-8169    | HIGH     | 7.64.0-4+deb10u1  |               | libcurl: partial passwor
           |                  |          |                   |               | leak over DNS on HTTP re
           |                  |          |                   |               | -->avd.aquasec.com/nvd/c
           +------------------+          +                   +---------------+-------------------
           | CVE-2020-8177    |          |                   |               | curl: Incorrect argument
           |                  |          |                   |               | check can allow remote s
           |                  |          |                   |               | to overwrite local files
           |                  |          |                   |               | -->avd.aquasec.com/nvd/c
           +------------------+          +                   +---------------+-------------------
           | CVE-2020-8231    |          |                   |               | curl: Expired pointer
           |                  |          |                   |               | dereference via multi AP
           |                  |          |                   |               | `CURLOPT_CONNECT_ONLY` o
           |                  |          |                   |               | -->avd.aquasec.com/nvd/c
           +------------------+          +                   +---------------+-------------------
           | CVE-2020-8285    |          |                   |               | curl: malicious FTP serv
           |                  |          |                   |               | trigger stack overflow w
           |                  |          |                   |               | CURLOPT_CHUNK_BGN_FUNCTI
```

Config

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

- https://github.com/guzhongren/Buildkite-Dashboard/runs/4081563022?check_suite_focus=true



deploy Y-BuildKite-Monitor

ys ago in 2m 29s

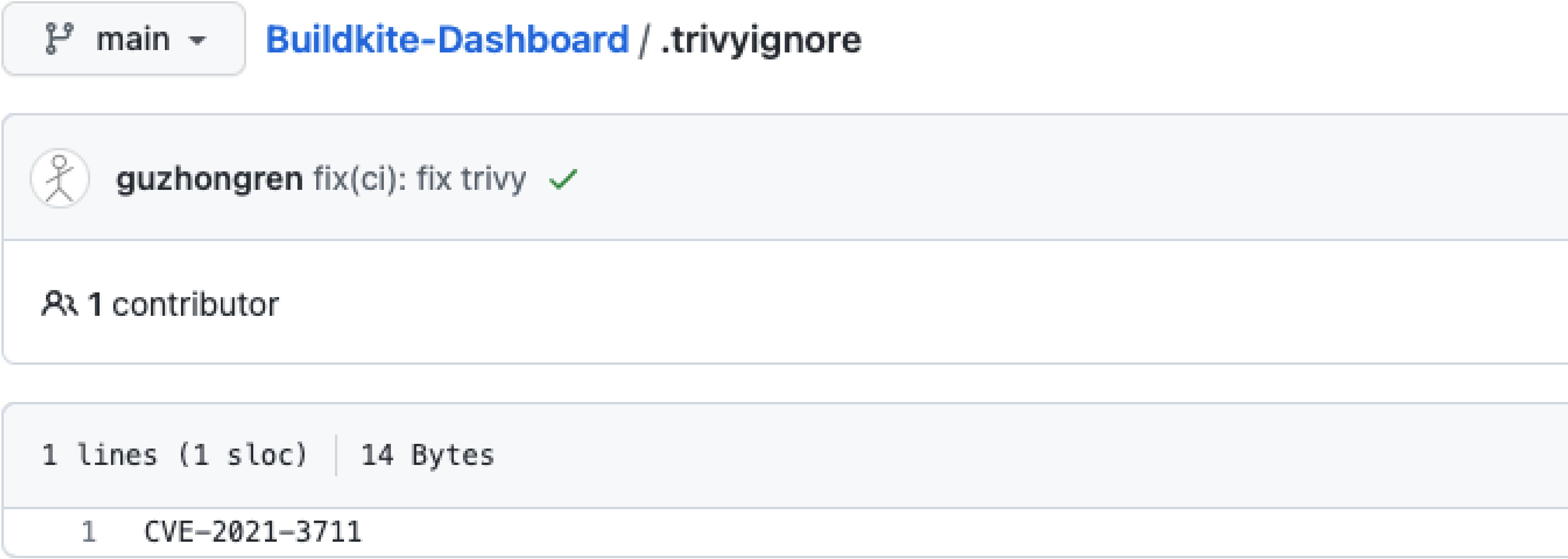
rivy scanner

```
ITHUB_PATH -e GITHUB_ENV -e RUNNER_OS -e RUNNER_TOOL_CACHE -e RUNNER_TEMP -e RUNNER_WORKSPACE -e ACTIONS_RUNT
ITHUB_ACTIONS=true -e CI=true -v "/var/run/docker.sock":"/var/run/docker.sock" -v "/home/runner/work/_temp/_g
/home/runner/work/_temp/_github_workflow":"/github/workflow" -v "/home/runner/work/_temp/_runner_file_command
ashboard/Buildkite-Dashboard":"/github/workspace" docker.io/aquasec/trivy:latest  "image" "--format=table" "-
everity=CRITICAL,HIGH" "--output=" "dashboard:09934b1a5b3f47b1c076e059e056d303a5c1c07b"
021-01-18T14:57:15.313Z        INFO    Need to update DB
021-01-18T14:57:15.313Z        INFO    Downloading DB...
021-01-18T14:57:21.789Z        INFO    Detecting Debian vulnerabilities...
021-01-18T14:57:21.803Z        INFO    Trivy skips scanning programming language libraries because no support

ashboard:09934b1a5b3f47b1c076e059e056d303a5c1c07b (debian 10.7)
===================================================================
otal: 30 (HIGH: 29, CRITICAL: 1)

-----------+------------------+----------+-------------------+---------------+----------------------
  LIBRARY  | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |
-----------+------------------+----------+-------------------+---------------+----------------------
 curl      | CVE-2020-8169    | HIGH     | 7.64.0-4+deb10u1  |               | libcurl: partial passwor
           |                  |          |                   |               | leak over DNS on HTTP re
           |                  |          |                   |               | -->avd.aquasec.com/nvd/c
           +------------------+          +                   +---------------+----------------------
           | CVE-2020-8177    |          |                   |               | curl: Incorrect argument
           |                  |          |                   |               | check can allow remote s
           |                  |          |                   |               | to overwrite local files
           |                  |          |                   |               | -->avd.aquasec.com/nvd/c
           +------------------+          +                   +---------------+----------------------
           | CVE-2020-8231    |          |                   |               | curl: Expired pointer
           |                  |          |                   |               | dereference via multi AP
           |                  |          |                   |               | `CURLOPT_CONNECT_ONLY` o
           |                  |          |                   |               | -->avd.aquasec.com/nvd/c
           +------------------+          +                   +---------------+----------------------
           | CVE-2020-8285    |          |                   |               | curl: malicious FTP serv
           |                  |          |                   |               | trigger stack overflow w
           |                  |          |                   |               | CURLOPT_CHUNK_BGN_FUNCTI
```

.trivyignore

```
CVE-2021-3711
```

- https://github.com/guzhongren/Buildkite-Dashboard/blob/main/.trivyignore



Buildkite-Dashboard / .trivyignore

guzhongren fix(ci): fix trivy ✓

1 contributor

1 lines (1 sloc) | 14 Bytes

```
CVE-2021-3711
```

Refs

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

Q & A

Thank you!