Securing Docker on the Cheap

Part 2 - Vulnerabilities

fork(4)

About Me

- Possessor of many hats
- Currently at LO3 Energy
- Formerly of Autodesk
- This talk brought to you by the letter ‘A’

But first....

The whale in the room

Orchestration platform agnostic

MESOSPHERE
DC/OS
Amazon ECS

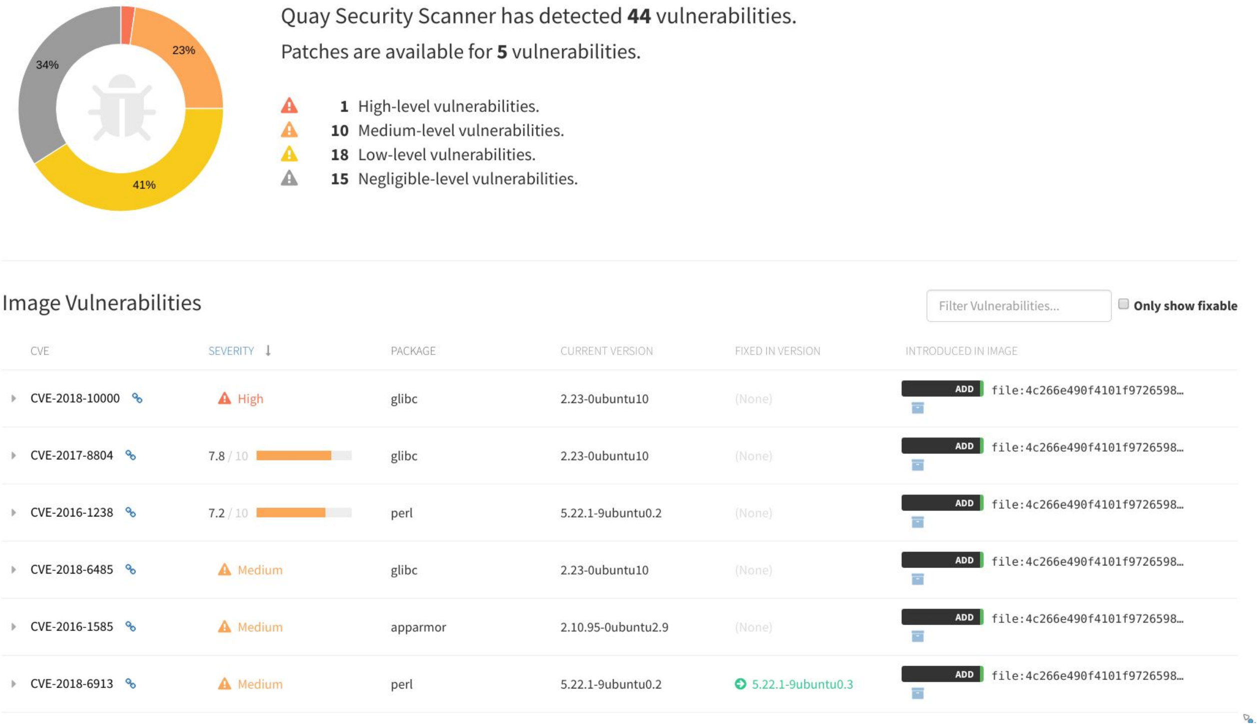
Solid Foundation

Security Starts at the Top

Sample Dockerfile

```
FROM ubuntu:16.04

RUN apt update && apt upgrade -y && apt install -y curl && \
   curl -sL https://deb.nodesource.com/setup_8.x | bash - && \
   apt install -y nodejs
EXPOSE 3000

ADD app.js /var/app/
ADD package.json /var/app/

WORKDIR /var/app
RUN npm install

CMD ["/usr/bin/node", "app.js"]
```

Security scan of ubuntu:16.04



Quay Security Scanner has detected **44** vulnerabilities.

Patches are available for **5** vulnerabilities.

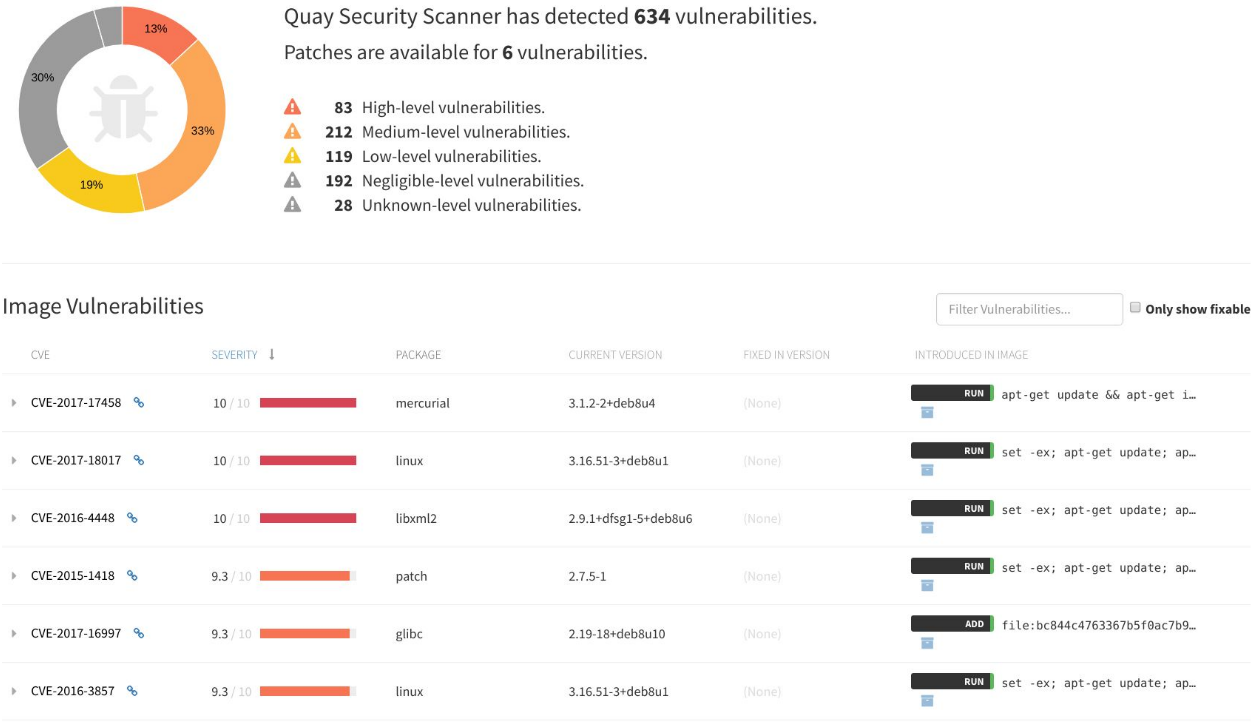
- **1** High-level vulnerabilities.
- **10** Medium-level vulnerabilities.
- **18** Low-level vulnerabilities.
- **15** Negligible-level vulnerabilities.

Image Vulnerabilities

Filter Vulnerabilities... □ **Only show fixable**

CVE	SEVERITY ↓	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN IMAGE
CVE-2018-10000	High	glibc	2.23-0ubuntu10	(None)	ADD file:4c266e490f4101f9726598...
CVE-2017-8804	7.8 / 10	glibc	2.23-0ubuntu10	(None)	ADD file:4c266e490f4101f9726598...
CVE-2016-1238	7.2 / 10	perl	5.22.1-9ubuntu0.2	(None)	ADD file:4c266e490f4101f9726598...
CVE-2018-6485	Medium	glibc	2.23-0ubuntu10	(None)	ADD file:4c266e490f4101f9726598...
CVE-2016-1585	Medium	apparmor	2.10.95-0ubuntu2.9	(None)	ADD file:4c266e490f4101f9726598...
CVE-2018-6913	Medium	perl	5.22.1-9ubuntu0.2	5.22.1-9ubuntu0.3	ADD file:4c266e490f4101f9726598...

Security scan of node:9.11.1



Quay Security Scanner has detected **634** vulnerabilities.

Patches are available for **6** vulnerabilities.

- **83** High-level vulnerabilities.
- **212** Medium-level vulnerabilities.
- **119** Low-level vulnerabilities.
- **192** Negligible-level vulnerabilities.
- **28** Unknown-level vulnerabilities.

Image Vulnerabilities

Filter Vulnerabilities... □ **Only show fixable**

CVE	SEVERITY ↓	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN IMAGE
CVE-2017-17458	10 / 10	mercurial	3.1.2-2+deb8u4	(None)	RUN `apt-get update && apt-get i…`
CVE-2017-18017	10 / 10	linux	3.16.51-3+deb8u1	(None)	RUN `set -ex; apt-get update; ap…`
CVE-2016-4448	10 / 10	libxml2	2.9.1+dfsg1-5+deb8u6	(None)	RUN `set -ex; apt-get update; ap…`
CVE-2015-1418	9.3 / 10	patch	2.7.5-1	(None)	RUN `set -ex; apt-get update; ap…`
CVE-2017-16997	9.3 / 10	glibc	2.19-18+deb8u10	(None)	ADD `file:bc844c4763367b5f0ac7b9…`
CVE-2016-3857	9.3 / 10	linux	3.16.51-3+deb8u1	(None)	RUN `set -ex; apt-get update; ap…`

Creating a Custom Base Container

Rules for a Quality Custom Base

- Starting tiny is better
- Patch as part of the build
- Build a shared service base
  - Install common tools
  - Install base runtime
- Leave the application specifics for downstream containers
- Leverage any hardening standards/tools for the OS
- Don’t setup a firewall - Docker networking takes care of this
- Install only what you need!

Pro-tip: `docker run -it [base-image]:[tag] /bin/sh` to experiment

Scratch Containers

- Docker images can be derived from tarballs
- Docker containers need a filesystem
- ...but that does not need to be a full base OS filesystem
- Docker images can be built directly
- `FROM scratch`
- Statically-linked executables (like Go) can be built directly into Docker images

Security Validation

INSPEC
BY CHEF

Validating Hardening Using InSpec

- InSpec is a compliance auditing system from the makers of Chef
- Compliance suites expressed in human-readable language
- Integrates with test-kitchen
- Can validate many different types of system
- For Docker, two main use cases
  - Validate/audit hardening work on containers
  - Verify compliance of Docker hosts
- The DevSec project is a great place to start https://github.com/dev-sec

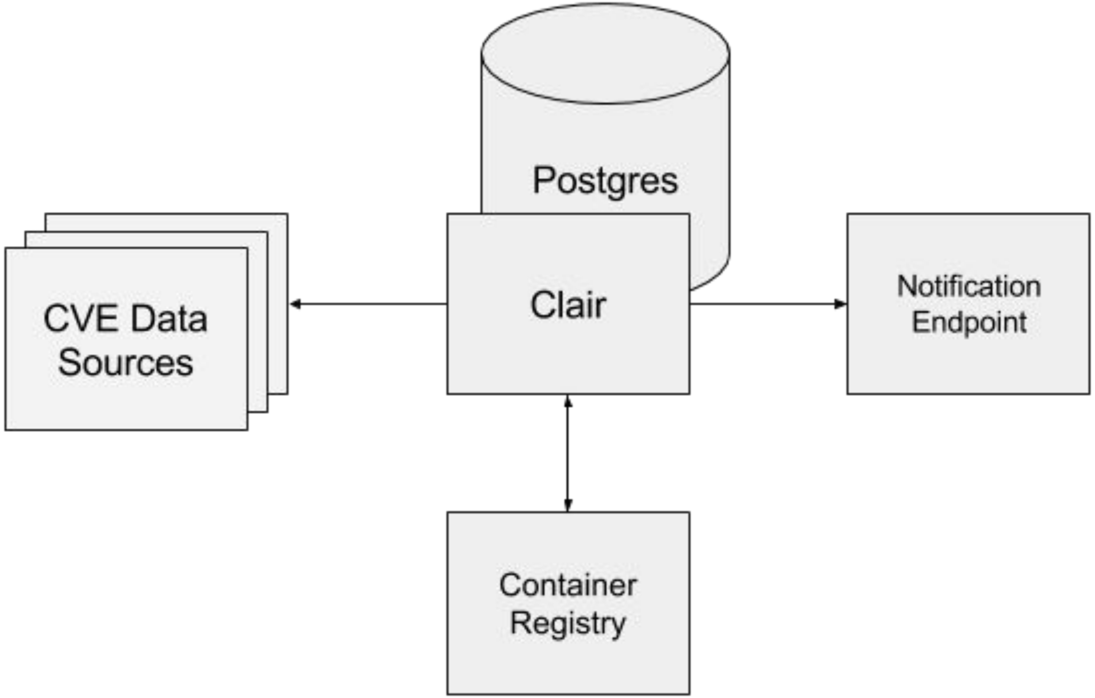
Demo

Running InSpec On a Container

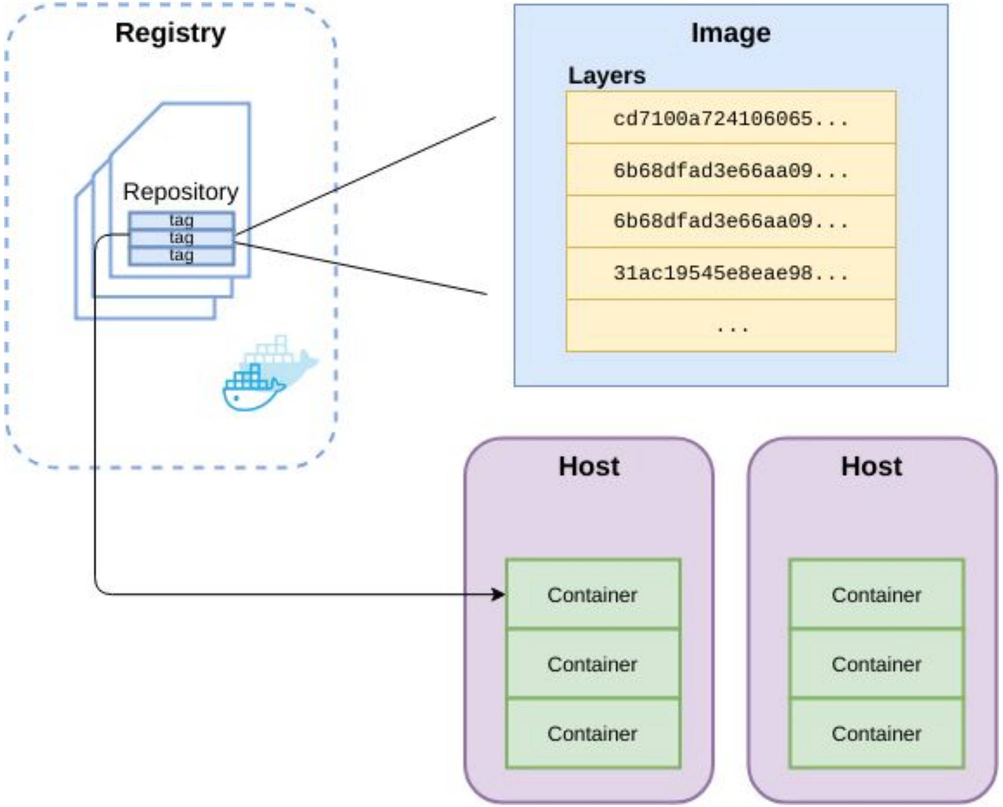
```
$ inspec exec https://github.com/dev-sec/linux-baseline -t
docker://ae344d0a573
...
Profile: DevSec Linux Security Baseline (linux-baseline)
Version: 2.2.0
Target:
docker://ae344d0a573c1e51767ad19cd4680d223bbc88e133f5e176037a33ae3a96db55
...
Profile Summary: 18 successful controls, 27 control failures, 9 controls
skipped
Test Summary: 44 successful, 47 failures, 12 skipped
```

clair

Clair Overview



Anatomy of a (Docker) Container



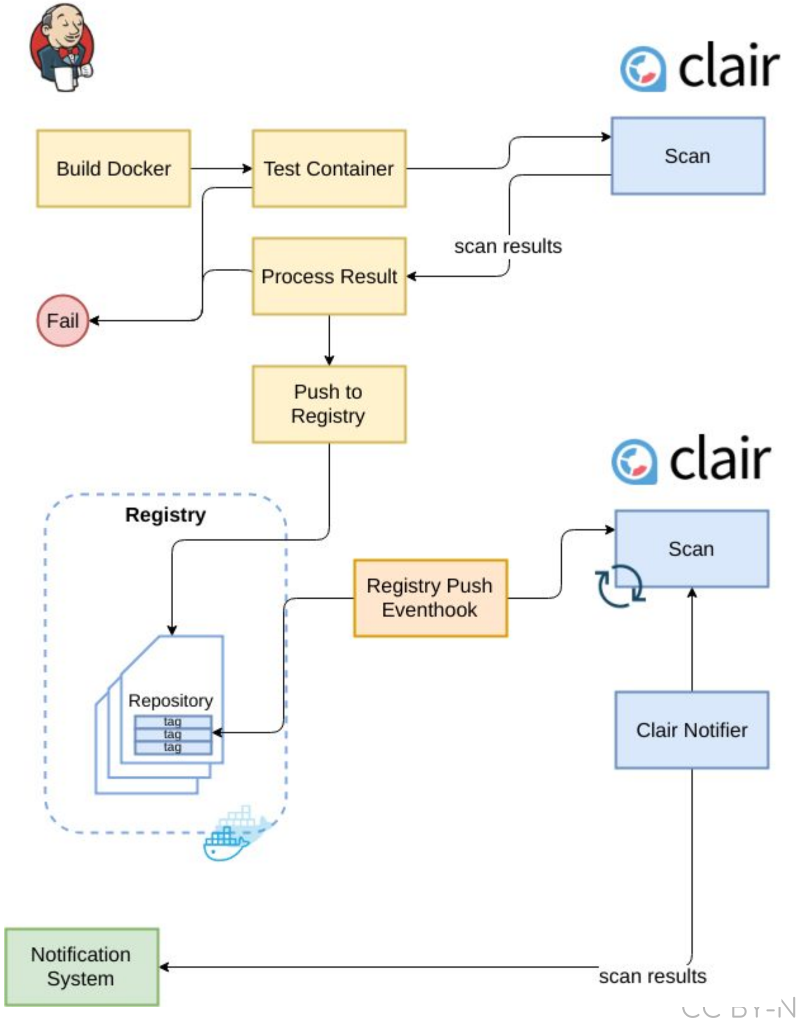
Demo

Docker Bench

What is Docker Bench?

- Benchmark security of a Docker host node
- Created and maintained by Docker
- Uses CIS inspired ruleset
- Can take custom rules

Vulnerability Lifecycle


clair
Build Docker
Test Container
Scan
scan results
Process Result
Fail
Push to Registry
clair
Registry
Scan
Registry Push Eventhook
Repository
tag
tag
tag
Clair Notifier
Notification System
scan results

Wrap-up

https://github.com/fork4/lfnw2018