Docker Container Security 101

@_gauravgahlot

$ whoami

https://gauravgahlot.in/

Gaurav Gahlot

Software Engineer @InfraCloud

Docker Community Leader & Tinkerbell Maintainer (CNCF) https://infracloud.io/careers/

What is container security?

Container Security

According to RedHat.

The protection of the integrity of containers.

This includes everything from the applications they hold to the infrastructure they rely on.

Containers

Containers are life savers.

Smoothen application development

Run just about anywhere

Attack Surfaces

Attack Surfaces

Flexibility comes at a cost.

Container

Images

Image Registries

Container Runtime

Orchestration Platforms

Host OS

Attack Surface

Container.

App Security

Scanning - docker-bench

Monitoring - Prometheus

Firewall - Cilium

Attack Surface

Images.

Up-to-date images

Image scanning (Clair)

Sign your images

DOCKER_CONTENT_TRUST=1

Attack Surface

Image Registries.

Private

Monitor vulnerabilities

Secure host server

Docker Hub - scanning, monitoring

Attack Surface

Container Runtime.

Tricky

Tools monitor container communication

Network protocols & payloads

Secure the Docker daemon

Host

Attack Surface

Orchestration Platforms.

Access control

Limit privileged users

Limit the privilege

Monitoring the platform

Monitoring pod/container communication

Attack Surface

Host OS.

Greatest vulnerability

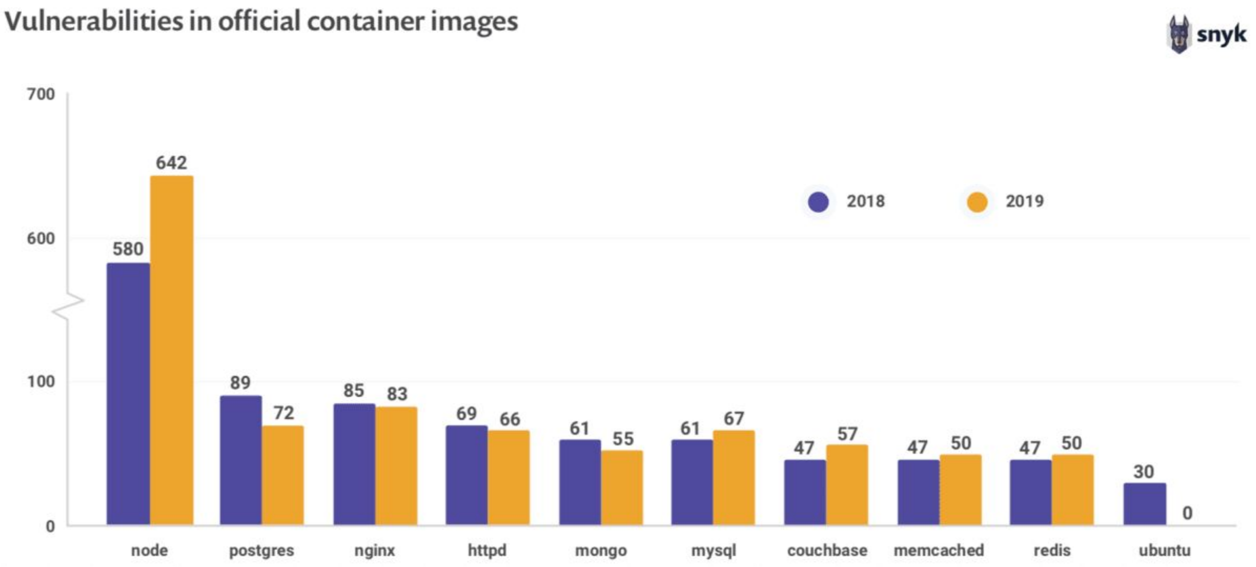
Updates

Slim OS - SE Linux

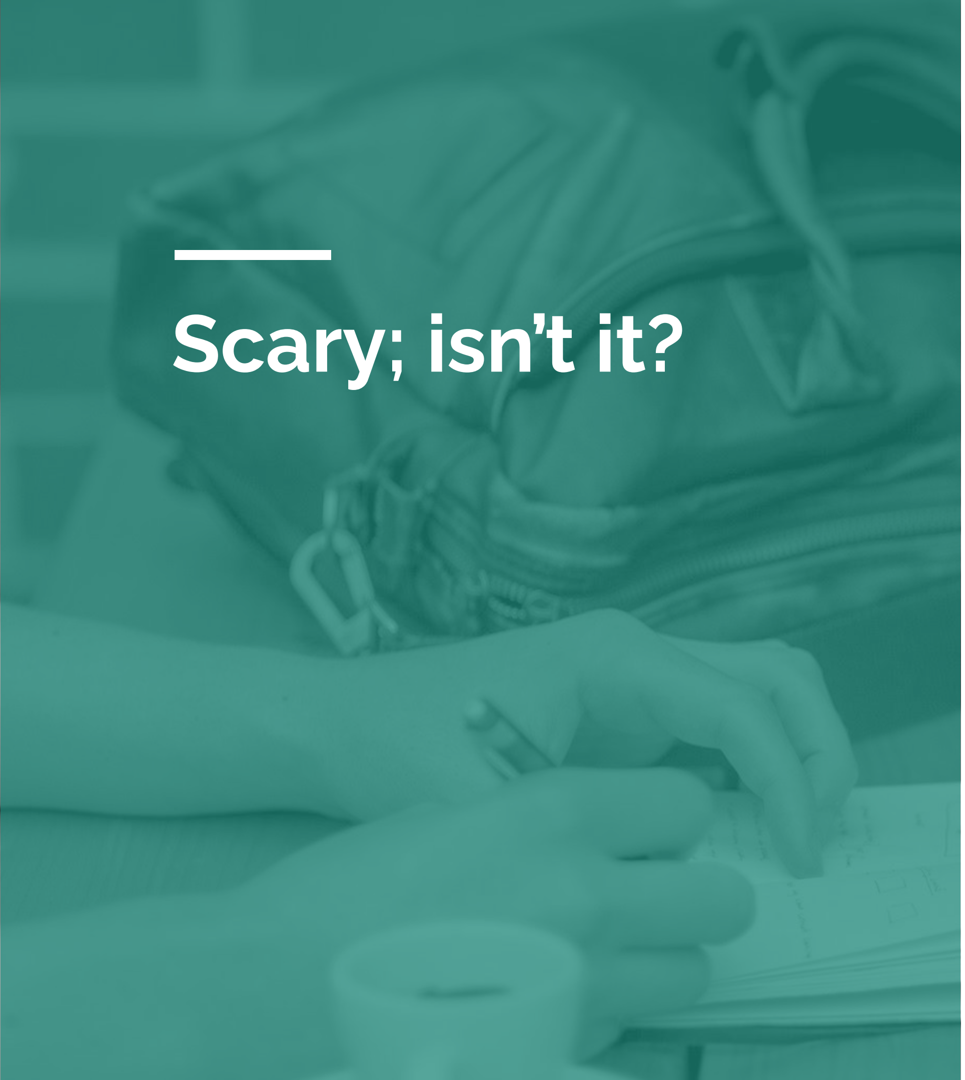
Access Control

Vulnerability scanning

The State of Open Source Security 2020



Source: *https://snyk.io/open-source-security/*



Scary; isn’t it?

Build Secure Docker Images

Dockerfile

Dockerfile best practices.

Minimal base image

Least privileged USER

Don’t ADD; COPY

RUN carefully

Multi-stage builds

Docker Runtime

Docker runtime best practices.

DOCKER_CONTENT_TRUST=1

Docker secrets

Publishing port(s) *-p <host-ip>:<port>*

Secure docker daemon --*tlsverify*

References

Docker Security Best Practices

Building Secure Docker Images

Dockerfile Best Practices

Thank you!

- ➔ https://gauravgahlot.in/
- ➔ Twitter - @_gauravgahlot
- ➔ LinkedIn - gauravgahlot
- ➔ GitHub - gauravgahlot