goto;

GOTO
AMSTERDAM 2023

#GOTOams

goto;

GOTO
Guide

LET US HELP YOU

Ask questions through **the app**

★★★★★

also remember to rate session

THANK YOU!

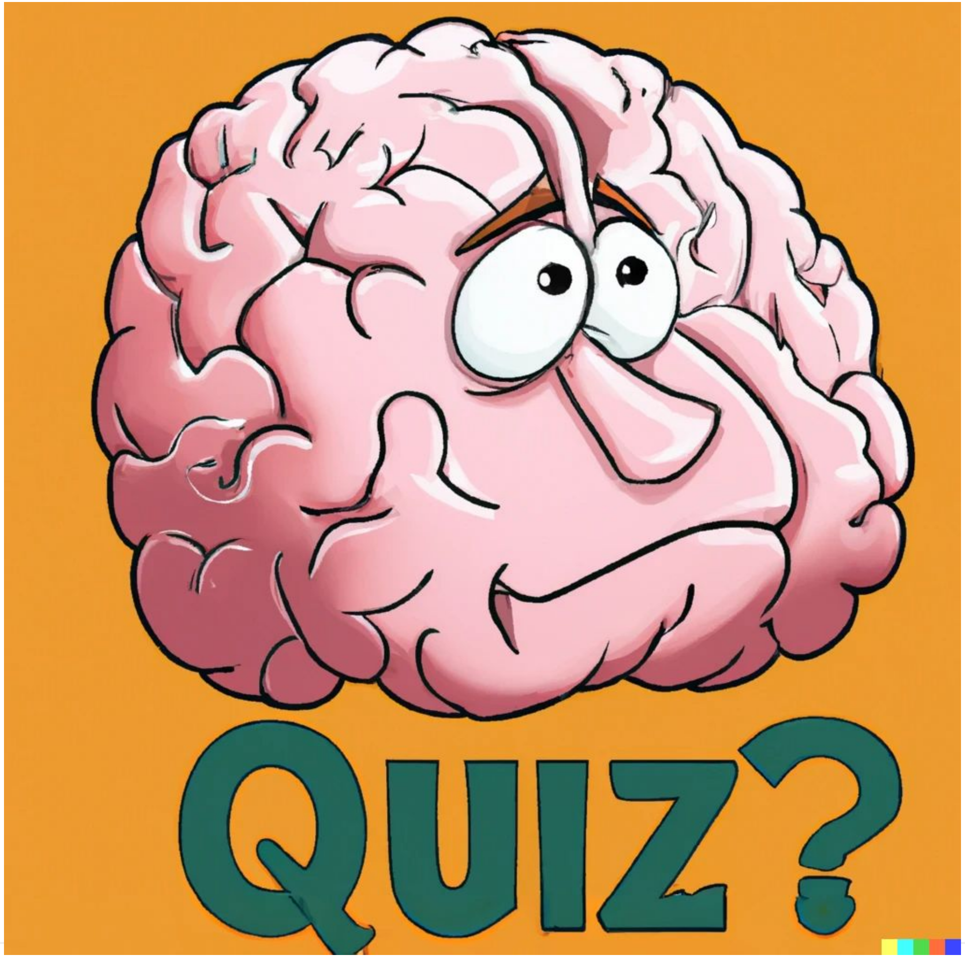
#GOTOams

Chainguard

Building Images for the Secure Supply Chain

Adrian Mouat
@adrianmouat

GOTO Amsterdam
June 29, 2023


QUIZ?

CVE-2017-5638

CVE-2017-5638

- Apache Struts RCE
    - Major factor in Equifax data breach
        - Private records compromised
            - 147.9m USA, 15.2m UK
        - Patch released March 7
        - Hack started March 12

CVE-2022-0847

CVE-2022-0847

- "Dirty Pipe"
  - Linux Kernel Vuln
  - Allows writing to read-only files
  - Privilege escalation
  - Android devices affected

CVE-2021-44228

CVE-2021-44228

- Log4shell
  - "the single biggest, most critical vulnerability ever"
  - "[saw] attempted attacks on over 40% of business networks internationally"
  - "hundreds of millions of devices [were vulnerable]"

CVE-2020-3716
CVE-2020-3717
CVE-2020-3718
CVE-2020-3719

CVE-2021-44228

- Magneto (MageCart)
  - ○

docker®

Vulnerability Scanners

HOUSTON
WE HAVE A PROBLEM...

```
$ grype nginx
 ✔ Vulnerability DB              [no update available]
 ✔ Loaded image
 ✔ Parsed image
 ✔ Cataloged packages            [151 packages]
 ✔ Scanning image...             [86 vulnerabilities]
   ├── 0 critical, 3 high, 4 medium, 4 low, 73
negligible (2 unknown)
   └── 2 fixed
```

```
$ grype node
 ✔ Vulnerability DB                [no update available]
 ✔ Loaded image
 ✔ Parsed image
 ✔ Cataloged packages              [682 packages]
 ✔ Scanning image...               [658 vulnerabilities]
   ├── 1 critical, 48 high, 124 medium, 30 low, 441
negligible (14 unknown)
   └── 4 fixed
```

artbleed Bug

d Bug is a serious vulnerability in the popular OpenSSL software library. This weakness allows stealing the otected, under normal conditions, by the SSL/TLS d to secure the Internet. SSL/TLS provides communication ivacy over the Internet for applications such as web, email, ing (IM) and some virtual private networks (VPNs).

d bug allows anyone on the Internet to read the memory of otected by the vulnerable versions of the OpenSSL compromises the secret keys used to identify the service o encrypt the traffic, the names and passwords of the ctual content. This allows attackers to eavesdrop ns, steal data directly from the services and users and to rvices and users.

SCAN

	Vulnerability	Severity	Package
>	CVE-2018-5709	Negligible	krb5
>	CVE-2018-7738	Negligible	util-linux
	CVE-2016-10228	Negligible	glibc
	VE-2019-7309	Negligible	glibc
	VE-2017-7245	Negligible	pcre3
	17-7246	Negligible	pcre3
	0654	Negligible	libtasn1-6
	[illegible]	Medium	krb5
	[illegible]	Medium	glibc
>	CV	Medium	libonig
>	CVE-2019-1	Medium	gnupg2

Redis (Debian Version)

```
$ grype redis:latest
 ✔ Vulnerability DB        [no update available]
 ✔ Loaded image
 ✔ Parsed image
 ✔ Cataloged packages      [100 packages]
 ✔ Scanning image...       [84 vulnerabilities]
   ├── 3 critical, 16 high, 4 medium, 9 low, 52 negligible
   └── 8 fixed
```

Redis (Alpine Version)

```
$ grype redis:alpine
 ✔ Vulnerability DB         [no update available]
 ✔ Loaded image
 ✔ Parsed image
 ✔ Cataloged packages       [20 packages]
 ✔ Scanning image...        [5 vulnerabilities]
   ├── 2 critical, 2 high, 0 medium, 1 low, 0 negligible
   └── 2 fixed
```

Redis (Chainguard Version)

```
$ grype cgr.dev/chainguard/redis
 ✔ Vulnerability DB         [no update available]
 ✔ Loaded image
 ✔ Parsed image
 ✔ Cataloged packages       [19 packages]
 ✔ Scanning image...        [0 vulnerabilities]
   ├── 0 critical, 0 high, 0 medium, 0 low, 0 negligible
   └── 0 fixed
```

AN A-PLUS!
HOW DID YOU DO IT?

Weirdly Simple

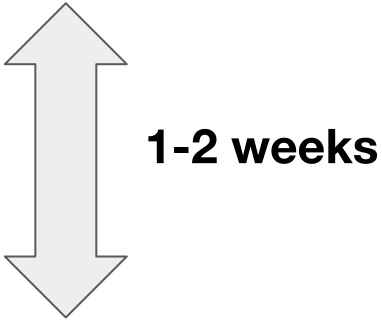
- Cut down dependencies
- Keep things up-to-date
- Apply patches when necessary

Cut Down Dependencies

- Debian has 100 packages
- Alpine has 20
- Wolfi has 19

Keep Things Up-To-Date

- Steps to fix a vuln
  - Vulnerability announced
  - Upstream releases patch
  - Distro releases new version
  - New image created



1-2 weeks

Wolfi

What is Wolfi

- An "Undistro"
  - Full package repo compiled from source
  - No kernel

What is Wolfi

- APK and glibc based
- Rolling releases
- SBOMs
- aarch64 and x86_64

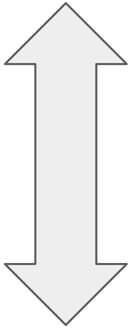
And Our Own Build Tooling

- Melange
  - Builds Wolfi packages
  - APK format

- Apko
  - Assembles APKs into Images
  - Reproducible
  - Declarative

Keep Things Up-To-Date

- Steps to fix a vuln
  - Vulnerability announced
  - Upstream releases patch
  - Distro releases new version
  - New image created



1-24 <u>Hours</u>

Applying Patches

- Upstream might not do a new release
  - Especially for transitive dependencies
- Need to tell scanners our version has a fix
- Enter security advisories!

Alpine Redis Vulnerabilities

```
NAME         INSTALLED  FIXED-IN   TYPE    VULNERABILITY   SEVERITY
libcrypto3   3.1.0-r4   3.1.1-r0   apk     CVE-2023-2650   High
libssl3      3.1.0-r4   3.1.1-r0   apk     CVE-2023-2650   High
redis        7.0.11                binary  CVE-2022-0543   Critical
redis        7.0.11                binary  CVE-2022-3647   Low
redis        7.0.11                binary  CVE-2022-3734   Critical
```

Wolfi Security Advisories

- YAML for Scanners
- https://github.com/wolfi-dev/advisories

Wolfi Security Advisory

```
package:
  name: redis

advisories:
  CVE-2022-0543:
    - timestamp: 2022-12-24T13:35:15-05:00
      status: fixed
      fixed-version: 7.0.7-r0
```

…

ABSOLUTELY NOTHING...

#SchittsCreek

Use Chainguard Application Images

- We have images for lots of stuff
  - Nginx, Redis, Vault, Prometheus, Postgres, RabbitMQ…
- https://github.com/chainguard-images/images

Use Smaller Base Images

- Alpine and Debian-slim
- Scratch
- Google Distroless
- Chainguard Base Images

Scratch

- Completely empty image
  - Great when it works
- But normally you need *some* OS stuff
  - ca-certificates, directory layout, users

Google Container Tools Distroless

- Much smaller than Debian or even Alpine
- No package manager or shell
- Limited number of images
- Hard to extend
  - Hope you like Bazel

Chainguard Base Images

- Similar to GCT distroless
- Easy to extend/customise
  - Apko or Dockerfile
- SBOMs included
- Continuously updated
- glibc support

Cut Down Dependencies

- Use multi-stage builds
- Separate dev or debug dependencies
- Pull in less libraries
    - Easier said than done…

Keep Updated

- Use tooling e.g. Dependabot
- "Build Horizon"
    - Idea from Google that all software must be continually rebuilt
    - So that container that's been running for 200 days…

Summary

- Use better images!
    - cough Chainguard cough
- Reduce Dependencies
- Keep S/W Updated
- And…

You Can Get to Zero!

References

- Chainguard Images
  - https://www.chainguard.dev/chainguard-images
  - https://github.com/chainguard-images/images
- Wolfi https://wolfi.dev
- Apko https://github.com/chainguard-dev/apko
- Melange https://github.com/chainguard-dev/melange
- Contact adrian@chainguard.dev

goto;

GOTO
Guide

★★★★★

Remember to **rate this session**

THANK YOU!

Download on the App Store

GET IT ON Google Play

#GOTOams