



Software Supply Chain Security

DataDog + Chainguard at Boston CSA

Patrick Smyth

Queens, New York

Staff DevRel at Chainguard

Python, Data Science at
James Webb, Columbia

patrick.smyth@chainguard.dev

@psmyth01 on X

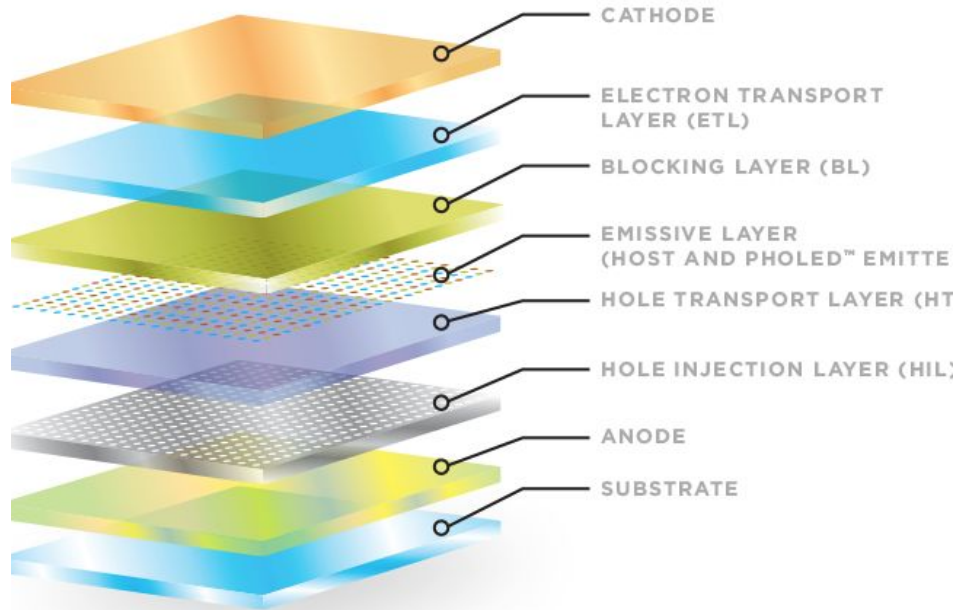


Physical Supply Chain

- Raw materials to finished product
- Complex network
- Many actors, many steps



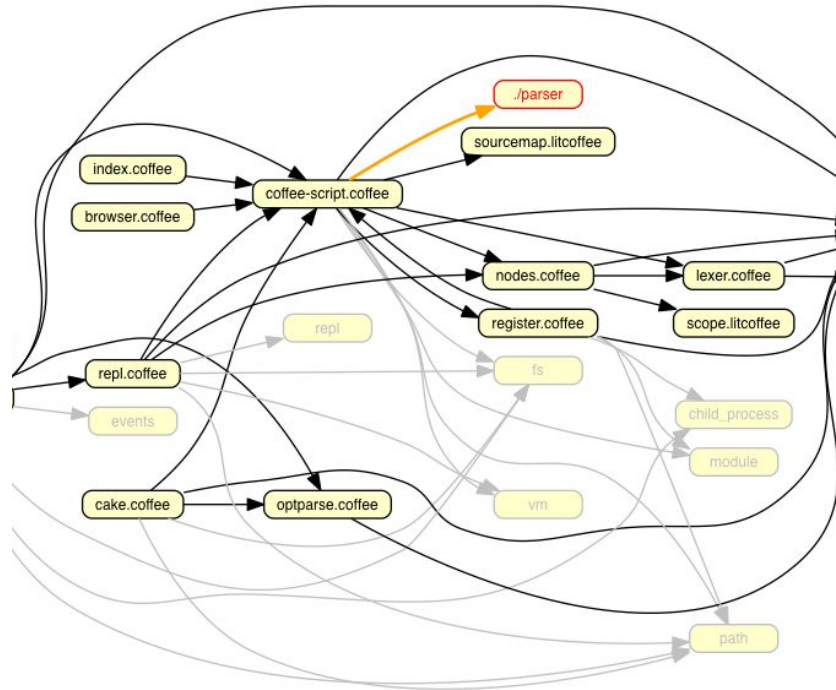
Interdependence



Transitive Dependencies



Software Supply Chain



- Software built on other software
- “Dependencies”
- Dependencies have dependencies

“Shift” Flows Downhill



Not Just Application Deps, sorry :(

Boss assigned me



TO FIX UBUNTU

CVE System



YOUR APP

CVEs



Who Tracks CVEs?

NLST

NVD

Who Tracks CVEs?



MITRE

Incidents



Solar Winds (90s Shareware on Floppy)

817

SOLAR WINDS

THE ESCAPE

Easy to use. Just type WIZ!
A Unique Game with Fast Arcade
Action and Outer-Space Role-
Playing Adventure!

THE #5 COMPUTER SOFTWARE STORE

EXCLUSIVELY FOR
IBM
AND COMPATIBLES

CONTAINS **3 1/2"** DISK

(Requires 256-Color VGA, 286 or
Better, 512K RAM & Hard Drive)



In a galaxy millions of light years from earth,
the survivors there await a solar system
disaster.



With the planet here to be
rescued, the planets of
this solar system are
you're... I've decided to
for... I've decided to
the system... I've
are... I've decided to
are... I've decided to

SELECT A RESPONSE

HAVE YOU?
HAVE YOU?
YOU ARE HERE, USE!
AND... I've decided to

YOU ARE BEING HAILED

ACTUAL SCREENS

Solar Winds (OG Supply Chain Hack)



SOLARWINDS®

CVE-2022-0847

“Dirty Pipe”

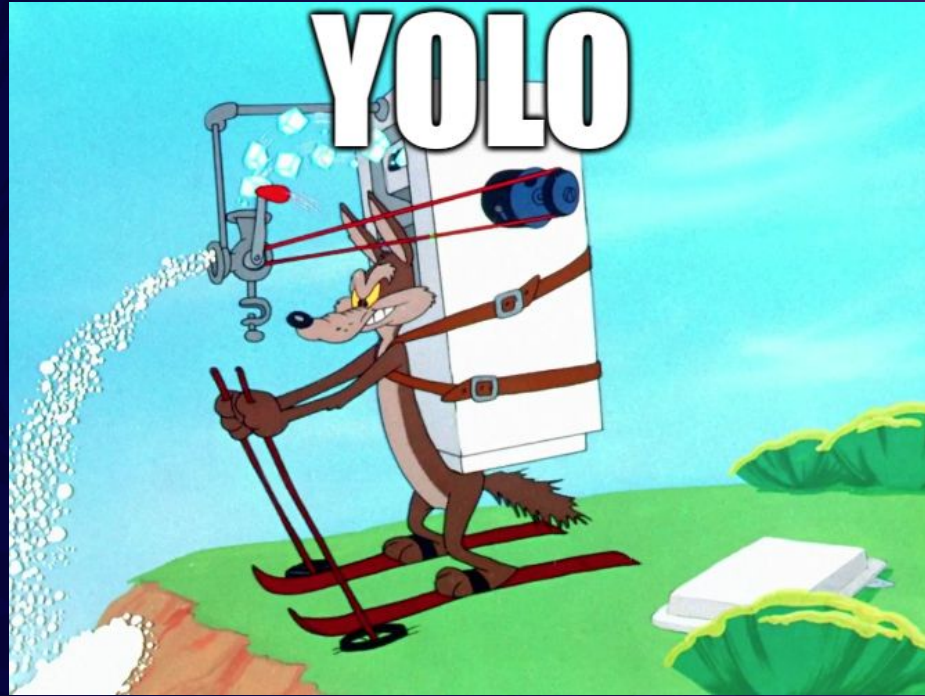
- Linux Kernel vulnerability
- Write to read-only files
- Privilege escalation
- Android devices affected
- “Catastrophic”

CVE-2021-44228

“Log4Shell”

- Arguably worst vulnerability of all time
- Attempted attacks on over 40% of world business networks
- Hundreds of millions of devices vulnerable

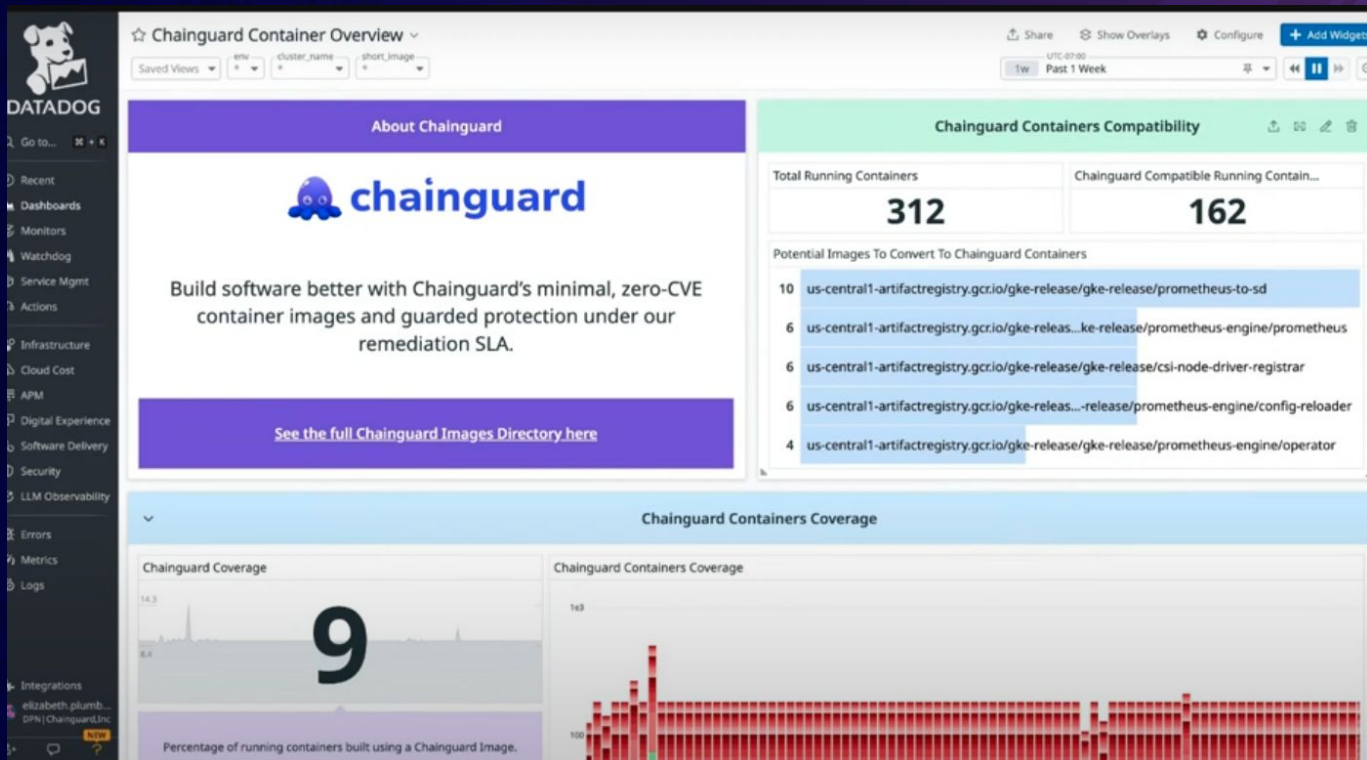
YOLO! (Ultralytix YOLO Attack)



SLSA



Observability (DataDog + Chainguard)



**HEAR ABOUT
SOFTWARE SUPPLY
CHAIN SECURITY**



**USE
SBOMS**



**SIGN WITH
SIGSTORE**



**USE
CHAINGUARD
LIBRARIES**



Chainguard Libraries

Chainguard Factory



Scanners



aqua
trivy



grype



snyk

Open Source Software Has Transformed Software Development

2%
Source Code

98%
Open Source



 python  Java

 GO  C  node.js

 cilium  MariaDB

 Grafana  kubernetes

DEMO TIME

Follow along on
go.chainguard.dev/introduction-supply-chain-demo

Software Supply Chain Security Principles



Resources

- ***NIST SP 800-161r1-upd1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations***
- ***NIST Special Publication 800-53 / Risk Assessment (RA)***
- ***Cybersecurity Supply Chain Risk Management C-SCRM***
- ***Security and Privacy Controls for Information Systems and Organizations***
- ***MITRE ATT&CK***





Goodbye!