Software Supply Chain

Understanding and Addressing Risk in OSS

Michael Winser - Google
Why Now?
Three Kinds of Security Attacks

- Front door
- Back door
- Underground
A very long time ago, Michael doesn't code anymore.
Software Supply Chain Risk
Correctness
Does the code have vulnerabilities that increase risk

Integrity
Has the code been modified from source to production

Availability
Is the code available to keep building software
What Could Possibly Go Wrong?
npm install foo
Upstream supply → Dependency management → Source management → Build → Publish → Release Management → Production footprint
Regress

Vulnerability management

Provenance, Audit and Enforcement

Source management

Build

Publish

Release Management

Dependency management

Policy

Upstream supply

Ingress

Transgress

Egress

Production footprint
What About Right Now?
Joint $5M investment by Microsoft and Google

Alpha: Direct research and engagement on top OSS projects
Omega: Scaled approach to the next 10,000 projects

Over $1.3M invested in Node, Python, Rust, Eclipse

10 Vulnerabilities reported, 50% fixed

~100 fully automated security reviews done against npm modules

Open source vulnerability detection toolkit
Resources

Scorecards: https://securityscorecards.dev/
Open Source Vulnerabilities: https://osv.dev/
Sigstore: https://www.sigstore.dev/
Open Source Insights: https://deps.dev/
OSS Fuzz: https://google.github.io/oss-fuzz/
Alpha Omega: https://opengsf.org/community/alpha-omega/
Alpha Omega Toolkit https://github.com/ossf/alpha-omega
DORA: https://cloud.google.com/devops/state-of-devops