

Dependency Management

Christian Köberl

twitter.com/derkoe github.com/derkoe



Christian Köberl



- Chief Technical Architect
- Entwickelt Software seit 1998
- Unterrichtet "Continuous Delivery" an der Fachhochschule Salzburg

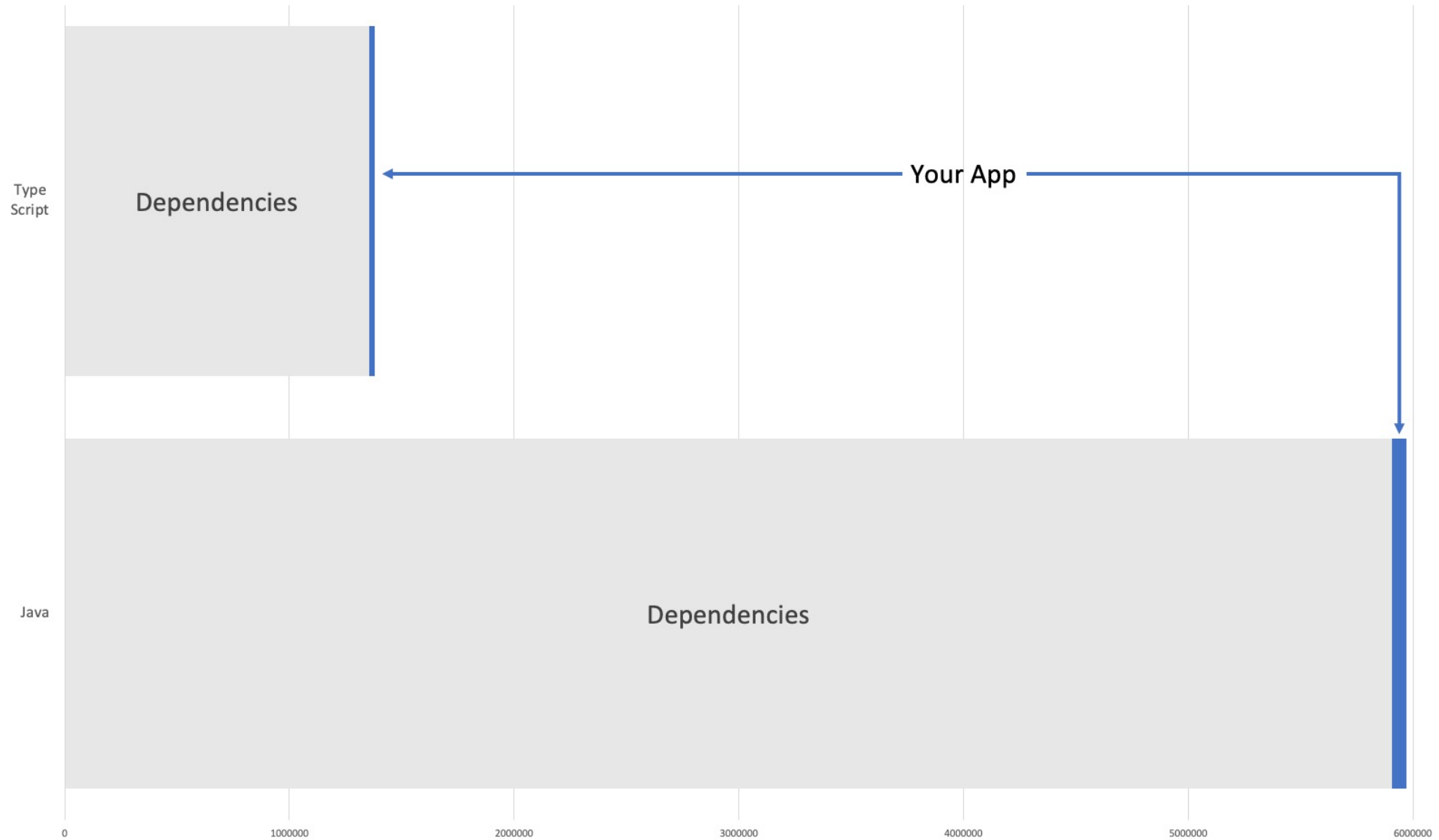
 twitter.com/derkoe

 github.com/derkoe

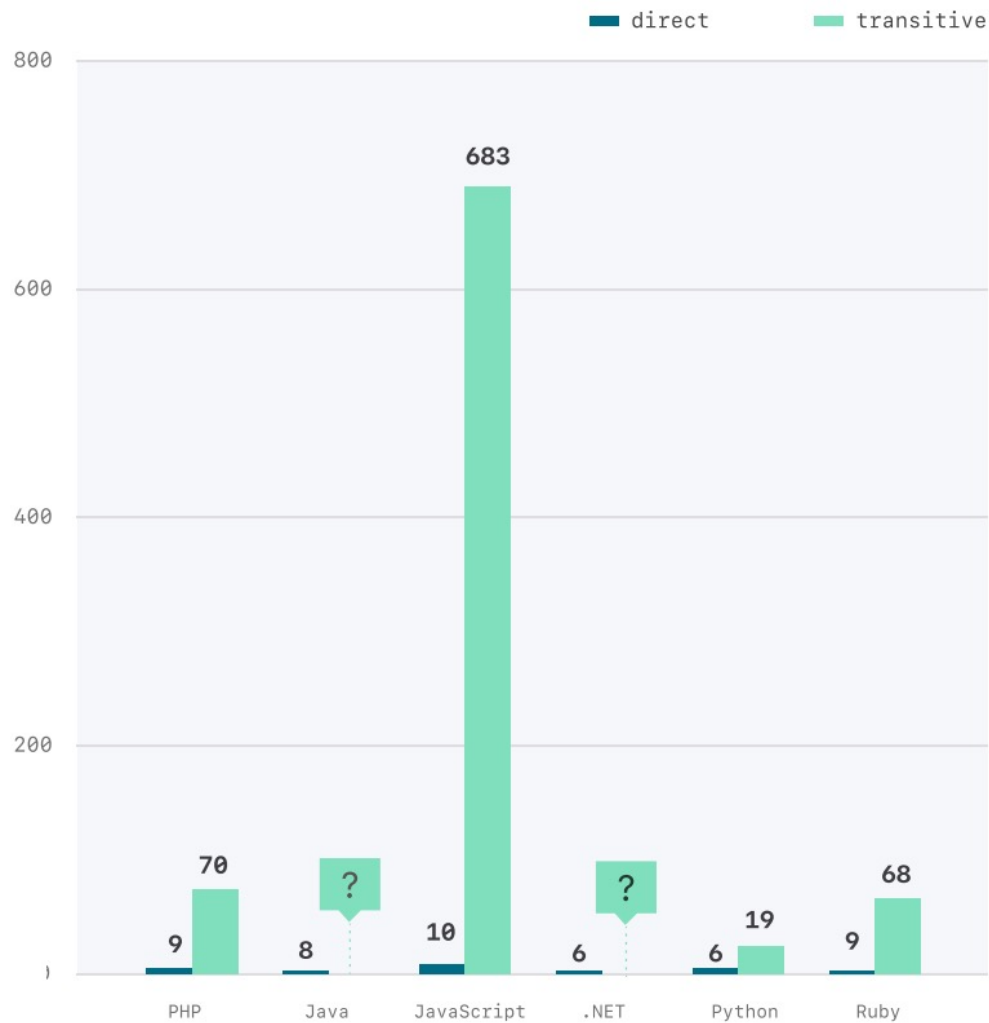
“If I have seen further
than others, it is by
standing on the
shoulders of Giants.”
– Isaak Newton



Your App vs Dependencies

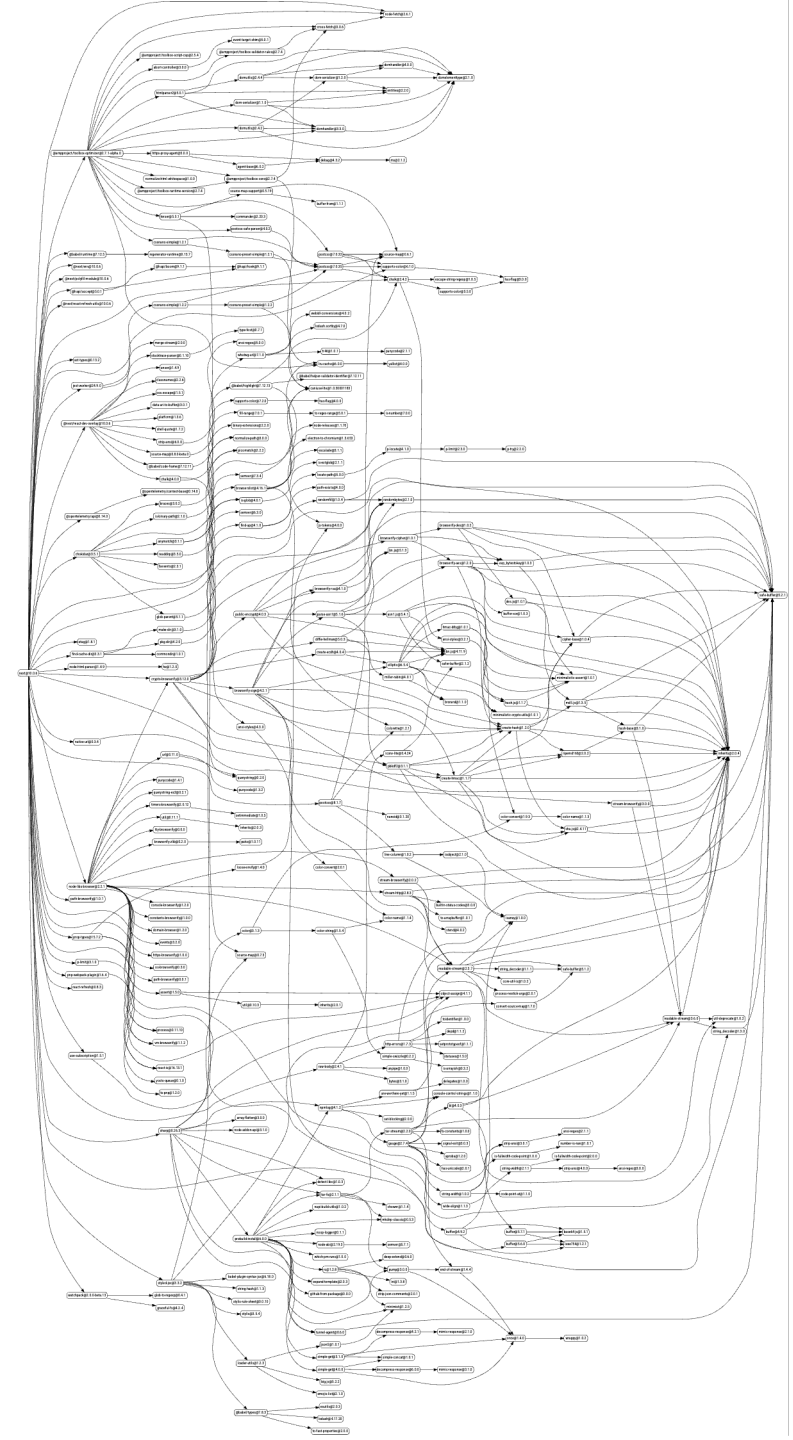


Median direct and transitive dependencies
per repository by package ecosystem

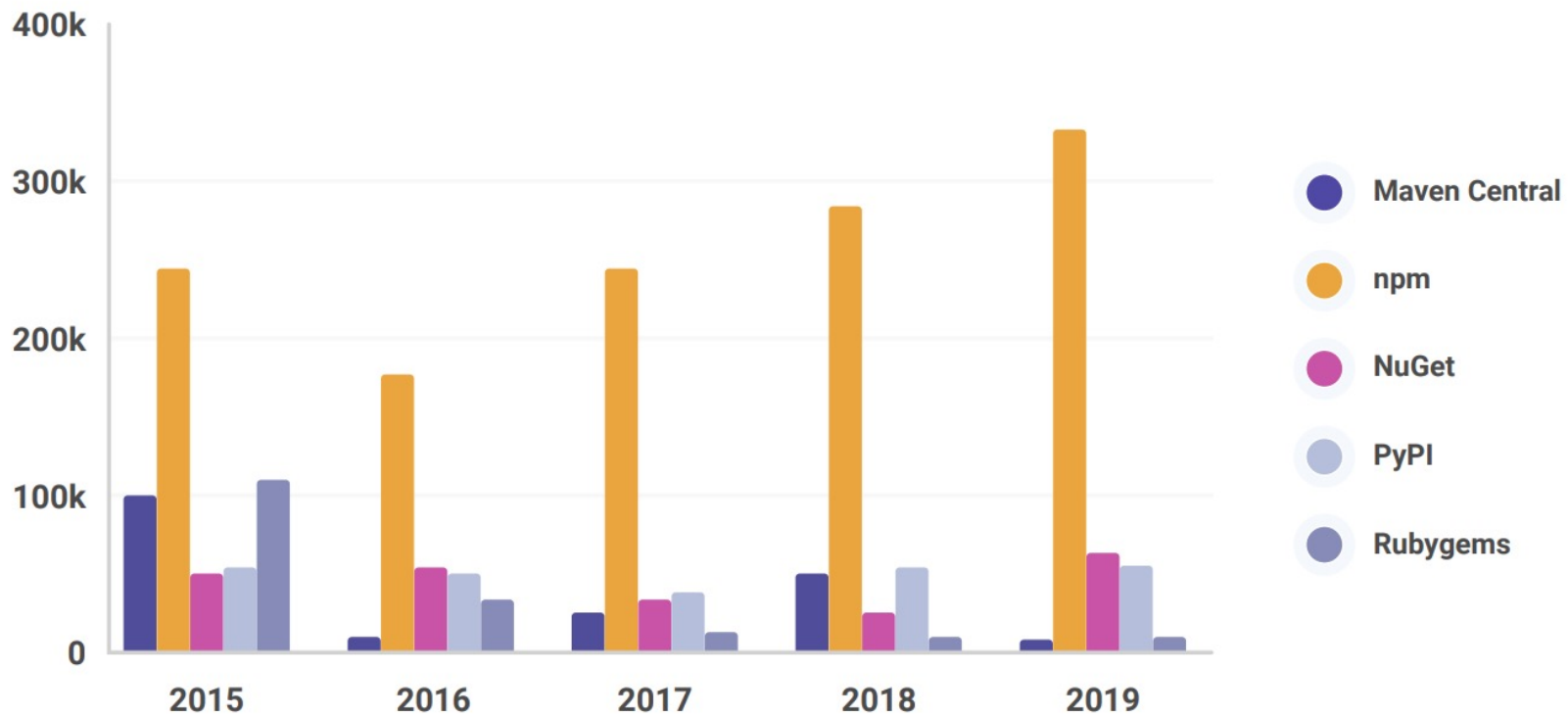


Dependency
Count

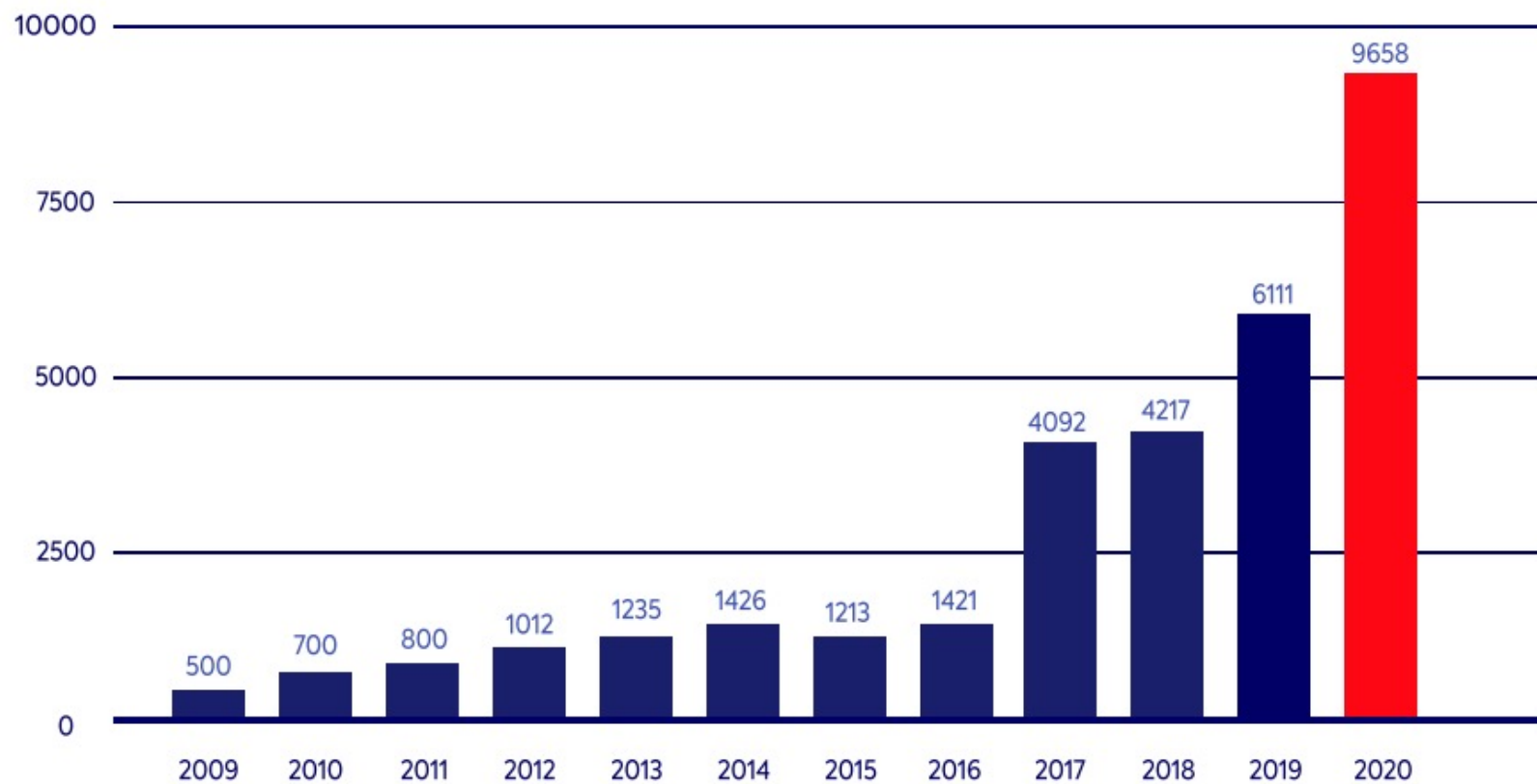
Next.js Dependency Graph



New packages created by ecosystem per year



Open Source
Libraries



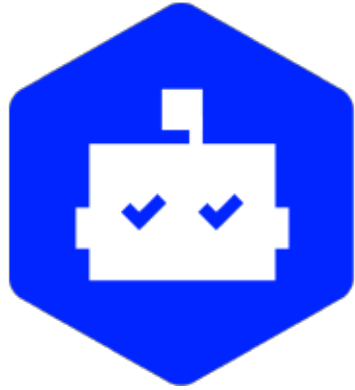
Vulnerabilities
increase

DevOps Tools - the
New Kids On the Block

Ansible
Terraform
Docker
Helm

...





Dependabot



Renovate

One Solution: Continuous Updates

Demo



Renovate



Open Source Health



npm

express

4.15.0 ▾

Overview

Dependencies

Dependents

Compare

Versions

Security Advisories

4

In the dependencies

Prototype Pollution Protection Bypass in qs

NO RATING

· GHSA-gqgv-6jq5-jjj9

[MORE DETAILS](#)

Regular Expression Denial of Service in debug

NO RATING

· GHSA-gxpj-cx7g-858c

[MORE DETAILS](#)

Regular Expression Denial of Service in fresh

NO RATING

· GHSA-9qj9-36jm-prpv

[MORE DETAILS](#)

Regular Expression Denial of Service in mime

NO RATING

· GHSA-wrvr-8mpx-r7pp

[MORE DETAILS](#)

Published

March 1, 2017

Description

Fast, unopinionated, minimalist web framework

Owners

doug@somethingdoug.comjasnell@gmail.commikeal.rogers@gmail.com

Links

<https://deps.dev/>

@angular/core

v12.2.9

Angular - the core framework

npm

NPM

📄

README

🌐

GitHub

📄

MIT

📅

Latest version published 6 days ago

```
npm install @angular/core
```

Explore Similar Packages

react

93 / 100

>

angular

83 / 100

>

cli

71 / 100

>

<https://snyk.io/advisor/>

KEEP YOUR PROJECT HEALTHY

IJ

Snyk Vulnerability Scanner

NEW

Get health score & security insights directly in your IDE

>

Secure Your Project

Make sure all the packages you're using are safe to use

Popularity

KEY ECOSYSTEM PROJECT

WEEKLY DOWNLOADS (2,869,619)

Download trend ▼

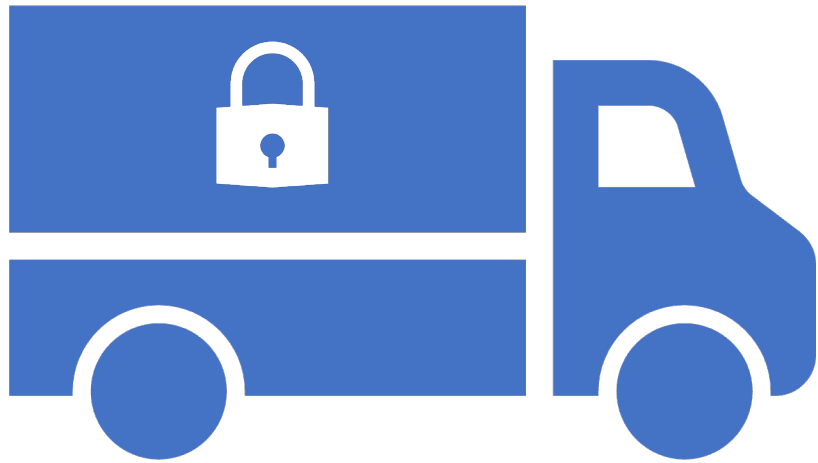


Maintenance

HEALTHY

COMMIT FREQUENCY





Supply Chain Security

A photograph of the Aurora Borealis (Northern Lights) in a dark night sky. The aurora appears as vibrant green, wavy bands of light. Numerous stars are visible in the background. At the bottom of the frame, a row of small, distant lights, possibly from a city or a spacecraft, is visible.

SolarWinds

Supply Chain Security



SLSA - slsa.dev

Supply-chain Levels for Software
Artifacts



Sigstore - www.sigstore.dev

Sign and verify signatures



CycloneDX - cyclonedx.org

Software Bill of Materials
(SBOM) Standard

Summary



Scan dependencies for known vulnerabilities



Automate dependency updates



Monitor the product/project health of your dependencies



Check fingerprints of your dependencies



Invest in reproducible builds

Sources

- Snyk: The State of Open Source Security 2020
<https://snyk.io/open-source-security/>
- Whitesource: The State of Open Source Security Vulnerabilities 2021
<https://www.whitesourcesoftware.com/wp-content/media/2021/04/the-state-of-open-source-vulnerabilities-2021.pdf>
- The 2020 State of the Octoverse
<https://octoverse.github.com/static/github-octoverse-2020-security-report.pdf#page=10>
- Mike McGarr (Netflix): Dependency Hell, Monorepos and beyond
<https://www.youtube.com/watch?v=VNqmHJtItCs>
- NPM Graph
<https://npm.broofa.com/>
- Microsoft: Analyzing Solorigate, the compromised DLL file that started a sophisticated cyberattack, and how Microsoft Defender helps protect customers
<https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/>
- Best practices for a secure software supply chain (Microsoft Docs)
<https://docs.microsoft.com/en-us/nuget/concepts/security-best-practices>
- Secure Developer Podcast: The CodeCov Breach
<https://www.devseccon.com/ep-102-the-codecov-breach/>