OPEN SECURITY SUMMIT

Dependency Management and Supply Chain Security

Christian Köberl

@derkoe
github.com/derkoe
derkoe.dev

Your next task is to figure out which applications in your org use log4j

OPEN SECURITY SUMMIT

Chief Technical Architect
at
PORSCHE INFORMATIK

Christian Köberl

twitter.com/derkoe

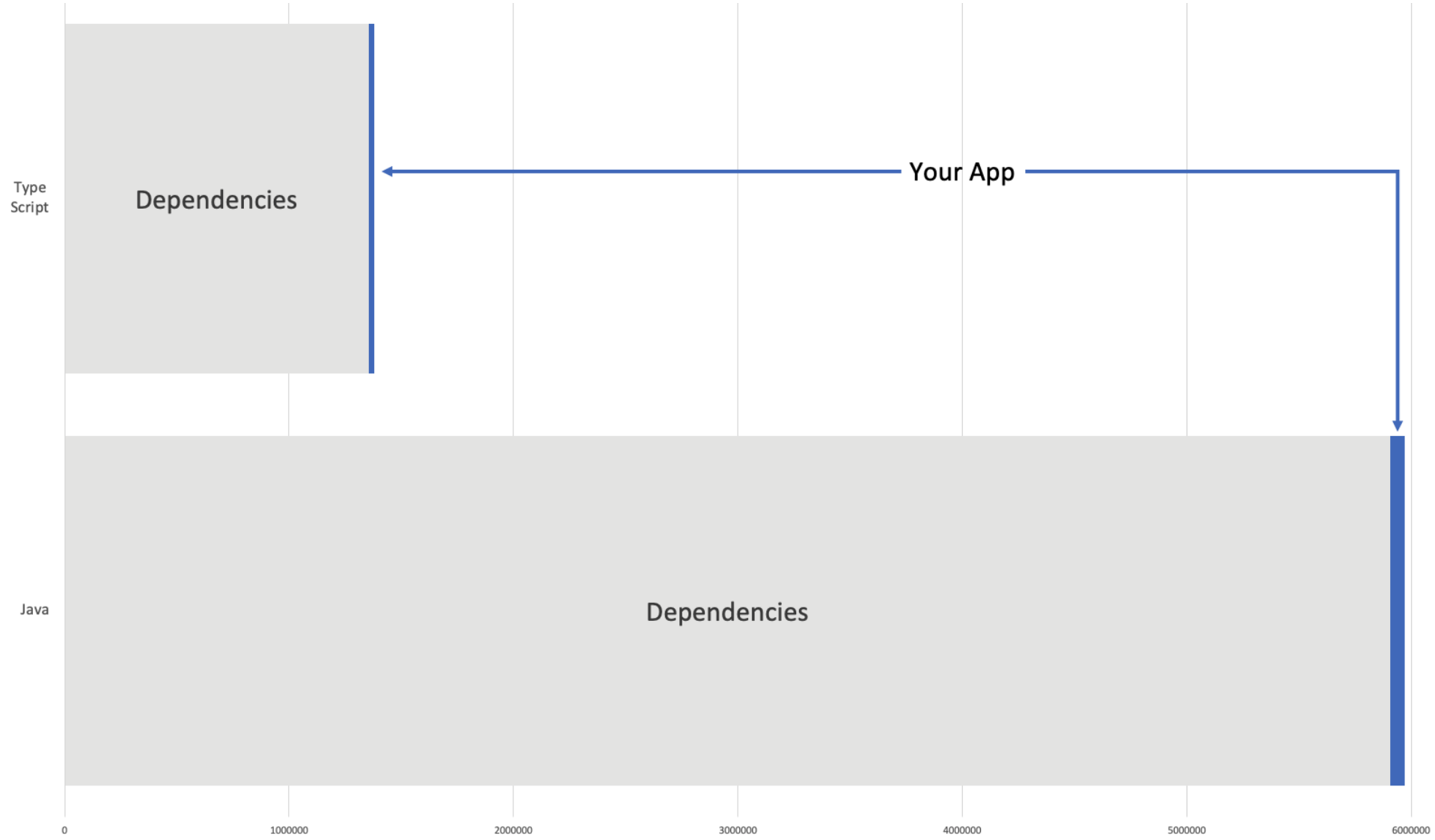
github.com/derkoe

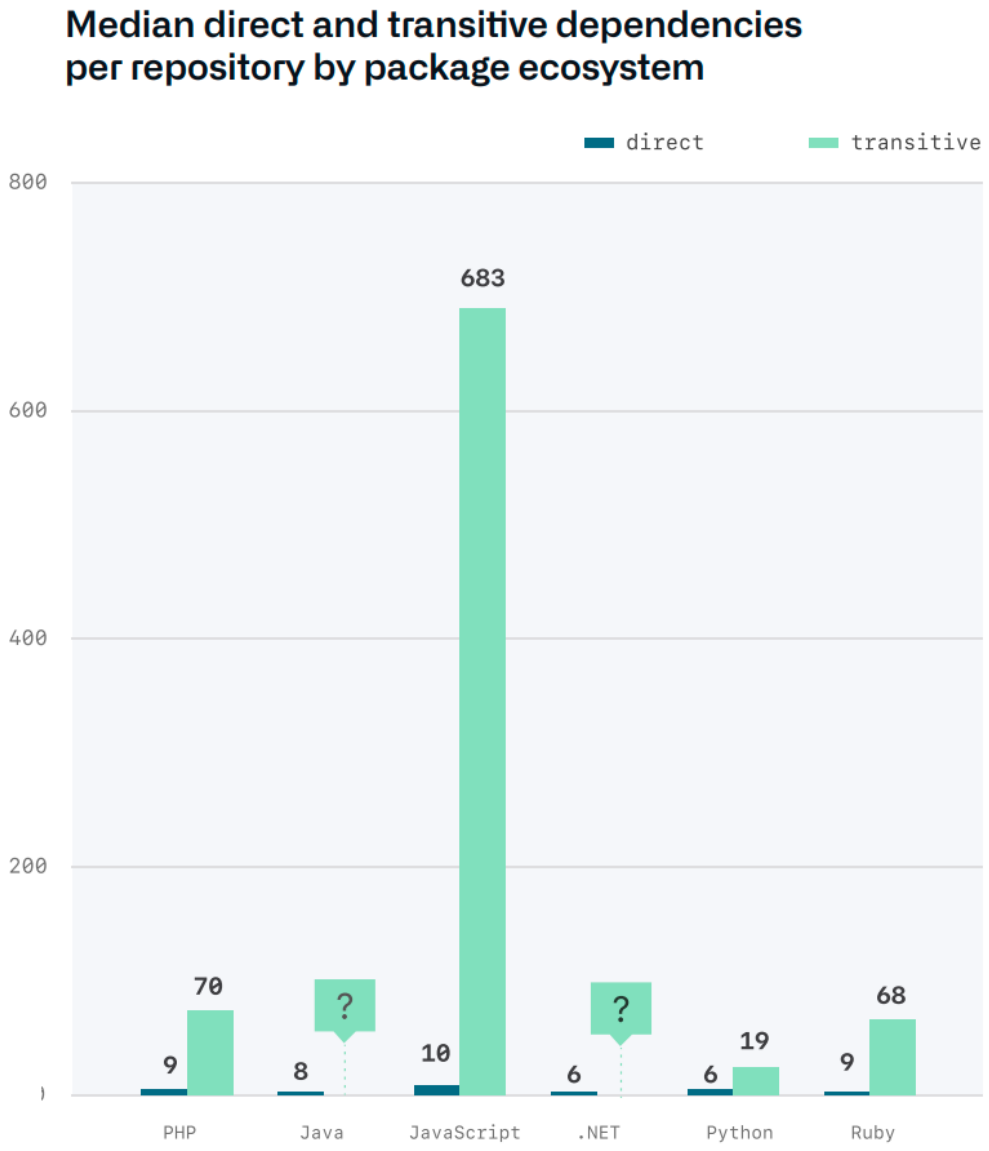
derkoe.dev

Professional software developer since 1998

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

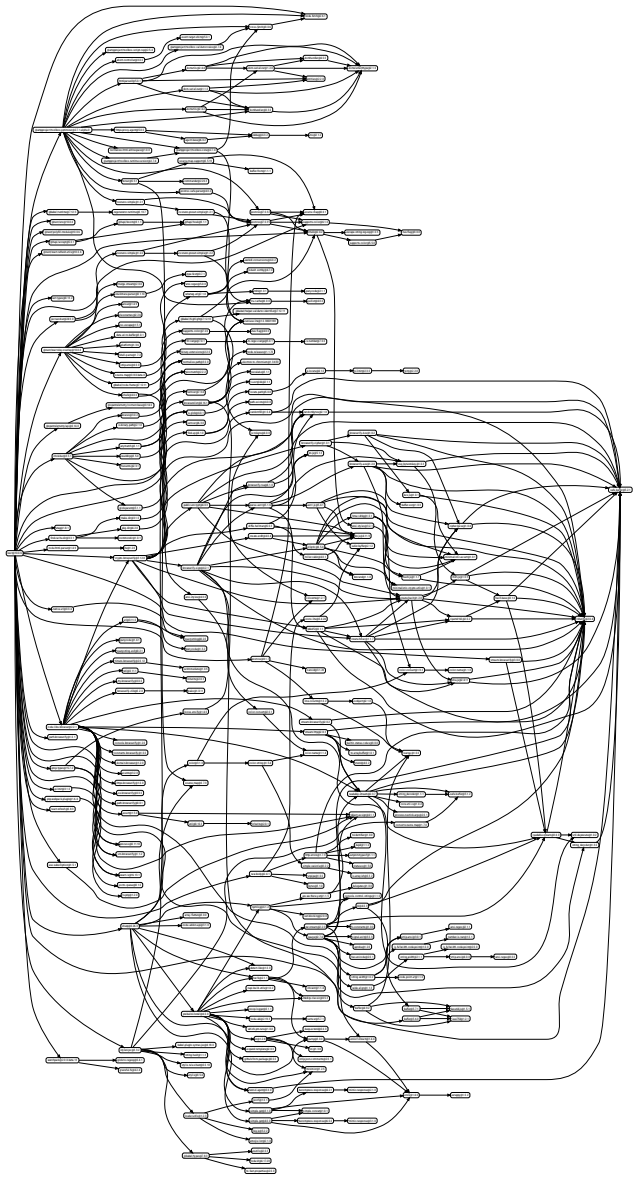
Your App vs Dependencies



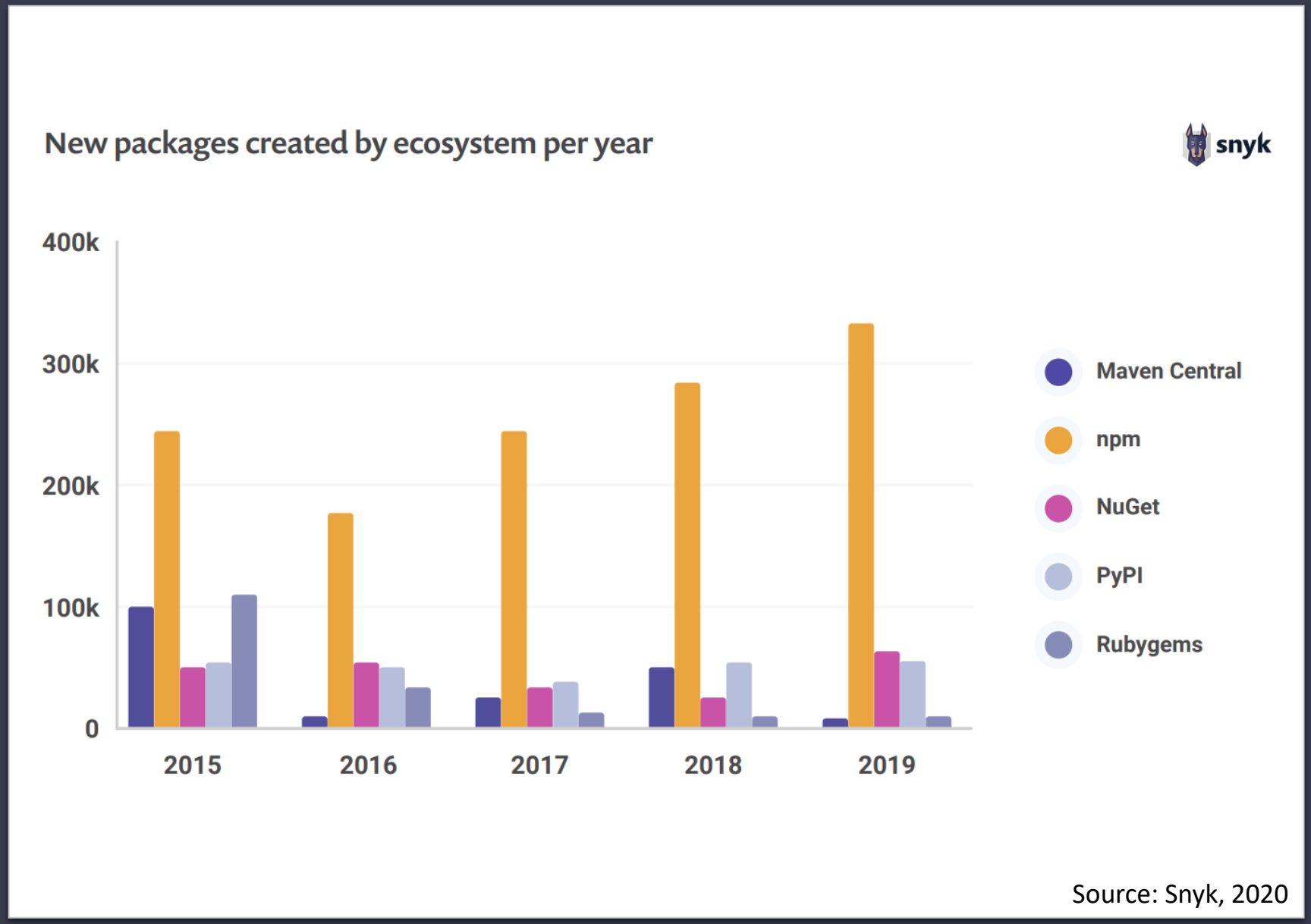


Dependency Count

Source: Snyk, 2020



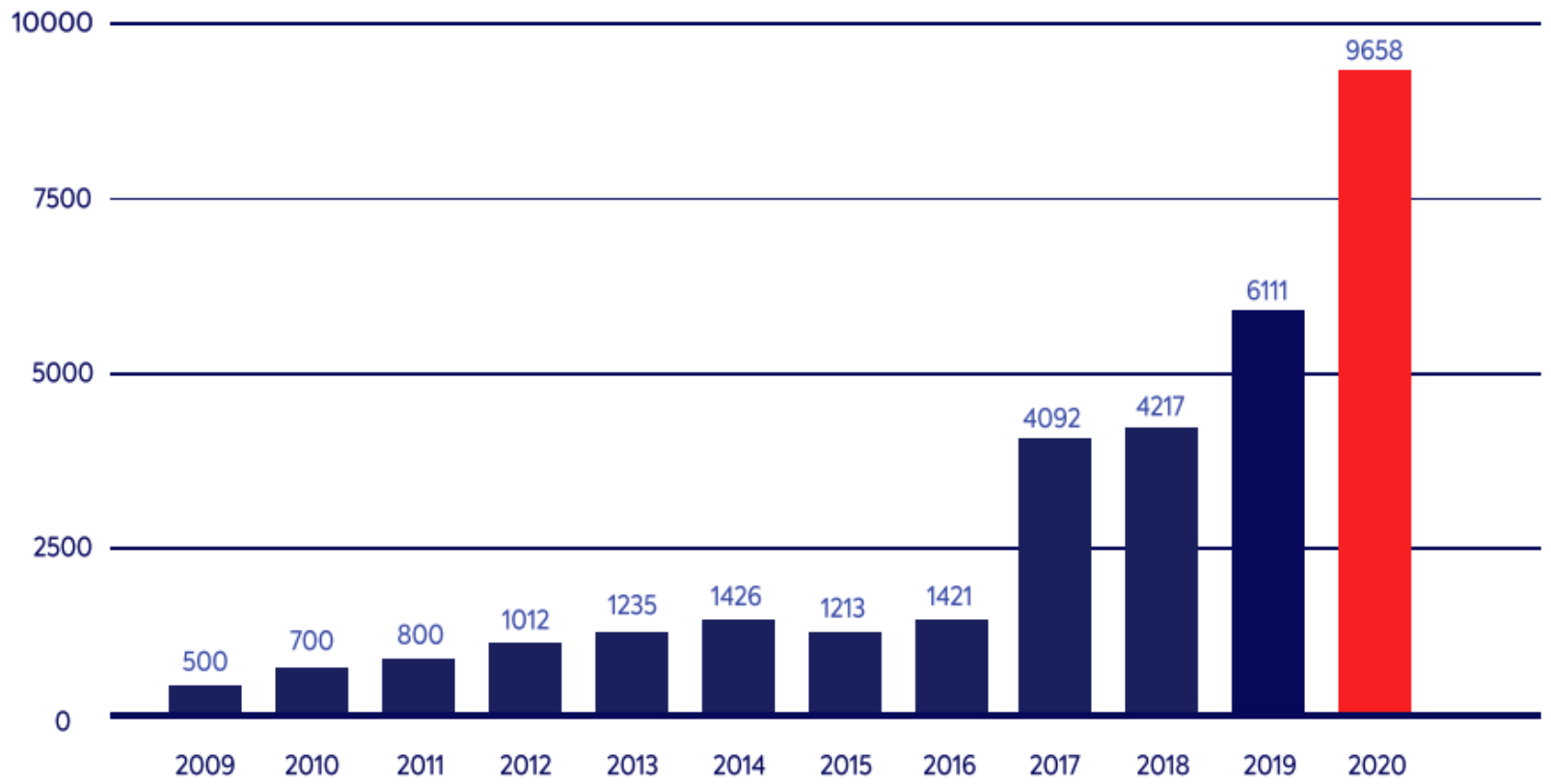
Next.js Dependency Graph



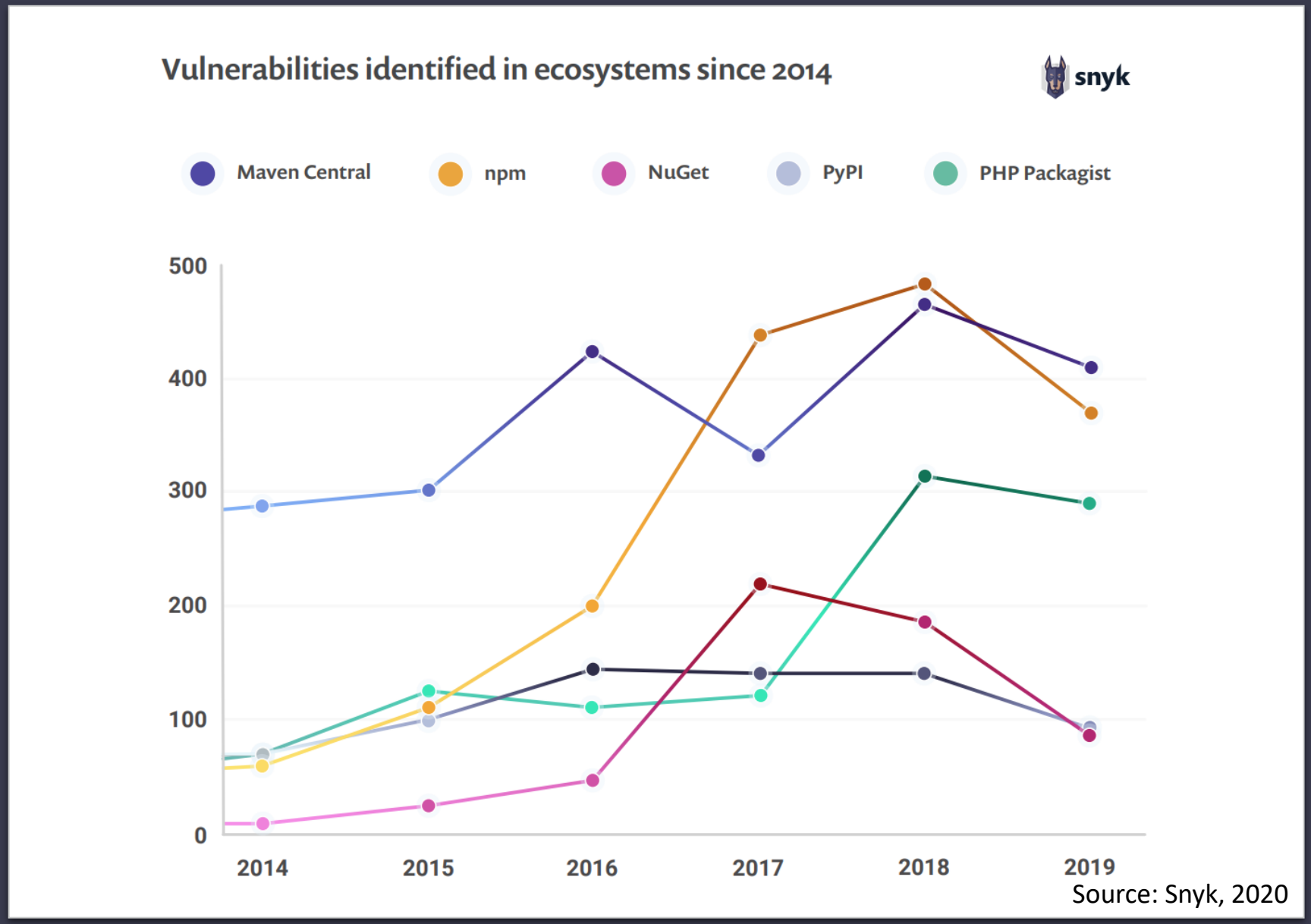
Source: Snyk, 2020

Lots of new packages

Vulnerabilities increase



Source: Whitesource, 2021

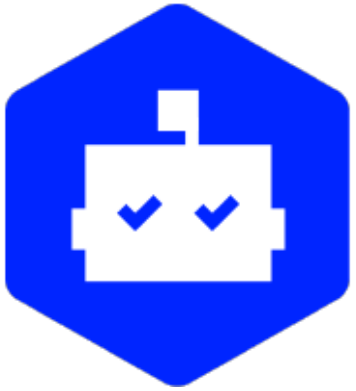


Source: Snyk, 2020

Open Source Vulnerabilites

DevOps Tools - the New Kids On the Block

Ansible
Terraform
Docker
Kubernetes
Helm
...



DependaBot

Renovate

One Solution: Continuous Updates

Demo

Renovate

Open Source Health

open / source / insights

Search for open source packages

npm

npm

express

4.15.0

Overview | Dependencies | Dependents | Compare | Versions

Security Advisories

4

In the dependencies

https://deps.dev/

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.com
jasnell@gmail.com
mikeal.rogers@gmail.com

Links

BETA

snyk Advisor | npm | Search packages | Open Source Basics | Code Securely | Categories | About Us | Sign Up

@angular/core v12.2.9

Angular - the core framework

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

Package Health Score

95 / 100

POPULARITY	KEY ECOSYSTEM PROJECT
MAINTENANCE	HEALTHY
SECURITY	NO KNOWN SECURITY ISSUES
COMMUNITY	ACTIVE

https://snyk.io/advisor/

KEEP YOUR PROJECT HEALTHY

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

Software Bill of Materials

What is a Software Bill Of Materials (SBOM)?

- List of all software components (aka dependencies)
- Including versions
- Including all transitive dependencies
- Usually also including the license

SBOM Standards

The Software Package Data Exchange® (SPDX®)

An open standard for communicating software bill of material information, including components, licenses, copyrights, and security references.

CycloneDX

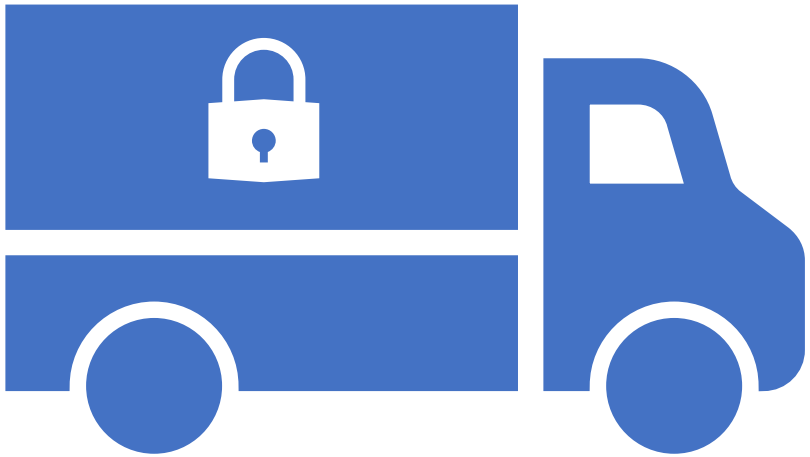
OWASP CycloneDX is a lightweight Software Bill of Materials (SBOM) standard designed for use in application security contexts and supply chain component analysis.

Demo

syft

grype

dependency track



Supply Chain Security

SolarWinds

Supply Chain Security

SLSA - https://slsa.dev/
Supply-chain Levels for Software Artifacts

Sigstore - https://www.sigstore.dev/
Sign and verify signatures

REACT

18.0.0 (latest)

Package Overview
Dependencies 1
Maintainers 7
Versions 874
Issues
File Explorer

ADVANCED TOOLS

NPM Scripts

react

React is a JavaScript library for building user interfaces.

18.0.0 latest

98 Supply Chain Security
84 Quality
99 Maintenance
100 Vulnerabilities

No tests

Package does not have any tests. This is a strong signal of a poorly maintained or low quality package.

Found in: react - package.json

https://socket.dev

Version published
4 weeks ago

Maintainers
7

Yearly downloads
644,430,814
▲ 43.88%

Weekly downloads
20.000.000
15.000.000
10.000.000
5.000.000
0

Changelog

18.0.0 (March 29, 2022)

Below is a list of all new features, APIs, deprecations, and breaking changes. Read React 18 release post and React 18 upgrade guide for more information.

New Features

React

- `useId` is a new hook for generating unique IDs on both the client and server, while avoiding hydration mismatches. It is primarily useful for component libra

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

OPEN SECURITY SUMMIT

🙏 Thank You! 🤣
Questsions?

@derkoe
github.com/derkoe
derkoe.dev

Software / Tools

- Renovate
  https://docs.renovatebot.com/ | https://www.whitesourcesoftware.com/free-developer-tools/renovate/on-premises/
- syft – CLI tool and library for generating a Software Bill of Materials
  https://github.com/anchore/syft
- grype – A vulnerability scanner for container images and filesystems
  https://github.com/anchore/syft
- OWASP Dependency Track
  https://dependencytrack.org/
- SBOM Operator
  https://github.com/ckotzbauer/sbom-operator
- Cosign
  https://docs.sigstore.dev/cosign/overview
- Socket
  https://socket.dev/
- Open Source Insights
  https://deps.dev/
- Snyk Advisor
  https://snyk.io/advisor/

Sources

- Snyk: The State of Open Source Security 2020
  https://snyk.io/open-source-security/
- Whitesource: The State of Open Source Security Vulnerabilites 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/
- SLSA (Supply-chain Levels for Software Artifacts)
  https://slsa.dev/
- Sigstore
  https://www.sigstore.dev/
- Best practices for a secure software supply chain (Microsoft Docs)
  https://docs.microsoft.com/en-us/nuget/concepts/security-best-practices