Health and Security of FOSS Supply Chain

Justin Chao

March 30, 2020

OPTUM®

Global Supply & Demand for FOSS

Global Supply & Demand for FOSS

The Economics of FOSS

80-90% of any given modern application is comprised of open source software.

Heavy reliance on FOSS is common in both the public and private sectors, tech and non-tech companies alike.

Ensuring the **health and security of FOSS Supply Chain is critical** to the future of nearly all industries in the modern economy.

OPTUM®

Global Supply & Demand for FOSS

Software Supply Chain

OPTUM®

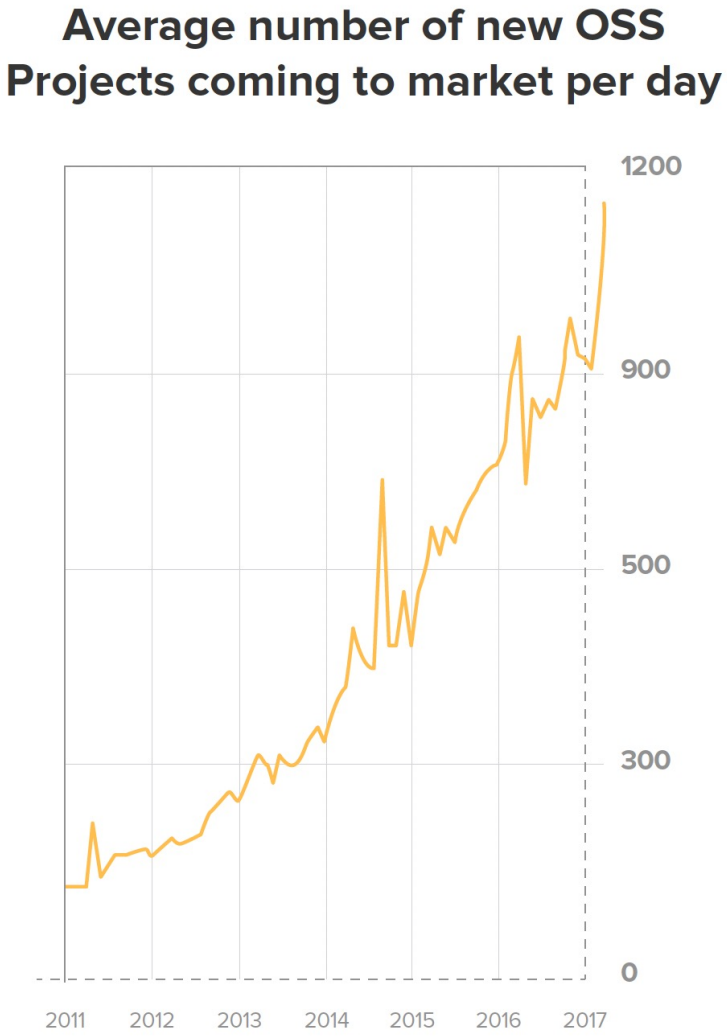
Global Supply & Demand for FOSS

Economics of FOSS

Today's development ecosystem is very complicated because of the **amount of components** out there.

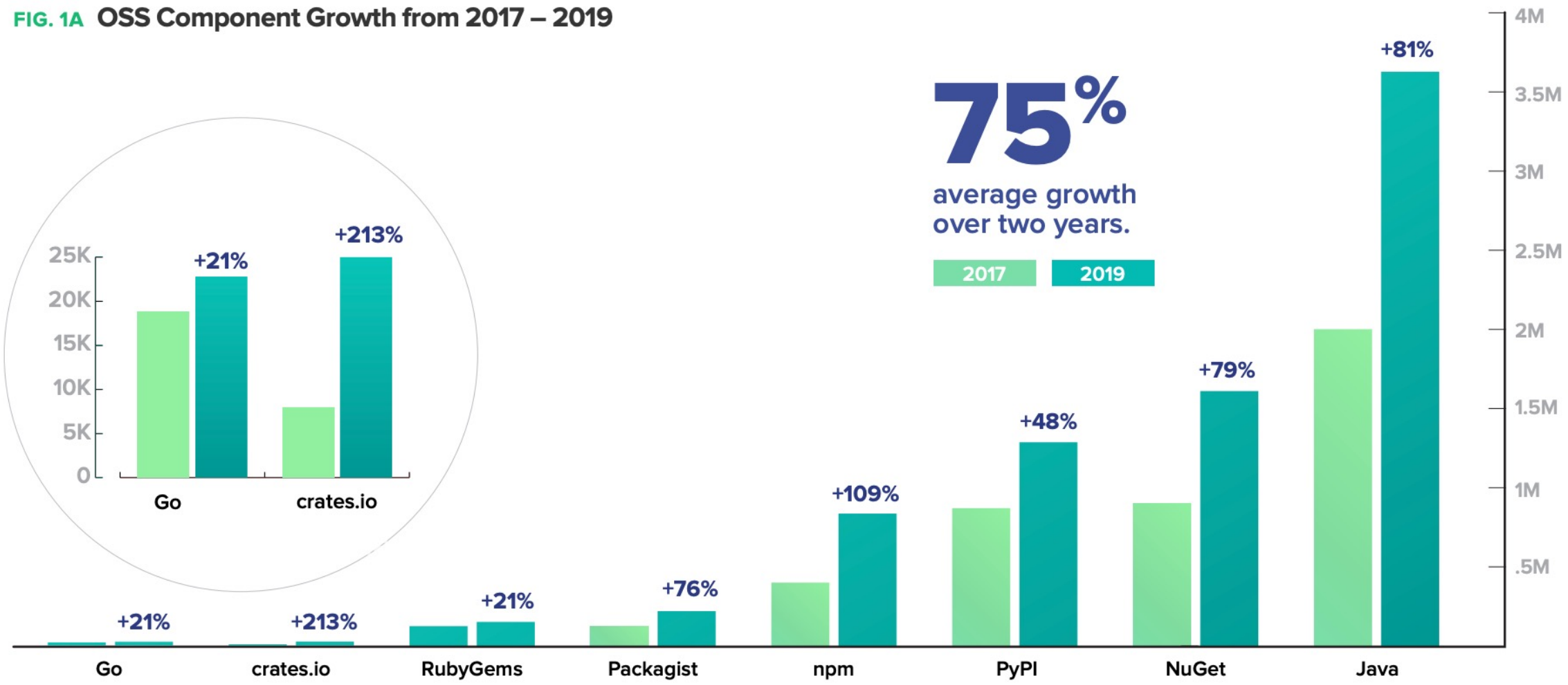
Most if not all components have **transitive dependencies**.

Number of OSS projects coming to market every day is **sharply increasing** each year.



OPTUM®

Global Supply & Demand for FOSS



OPTUM®

Global Supply & Demand for FOSS

FIG. 2A **Number of Download Requests for Java Component Releases 2012 – 2018**

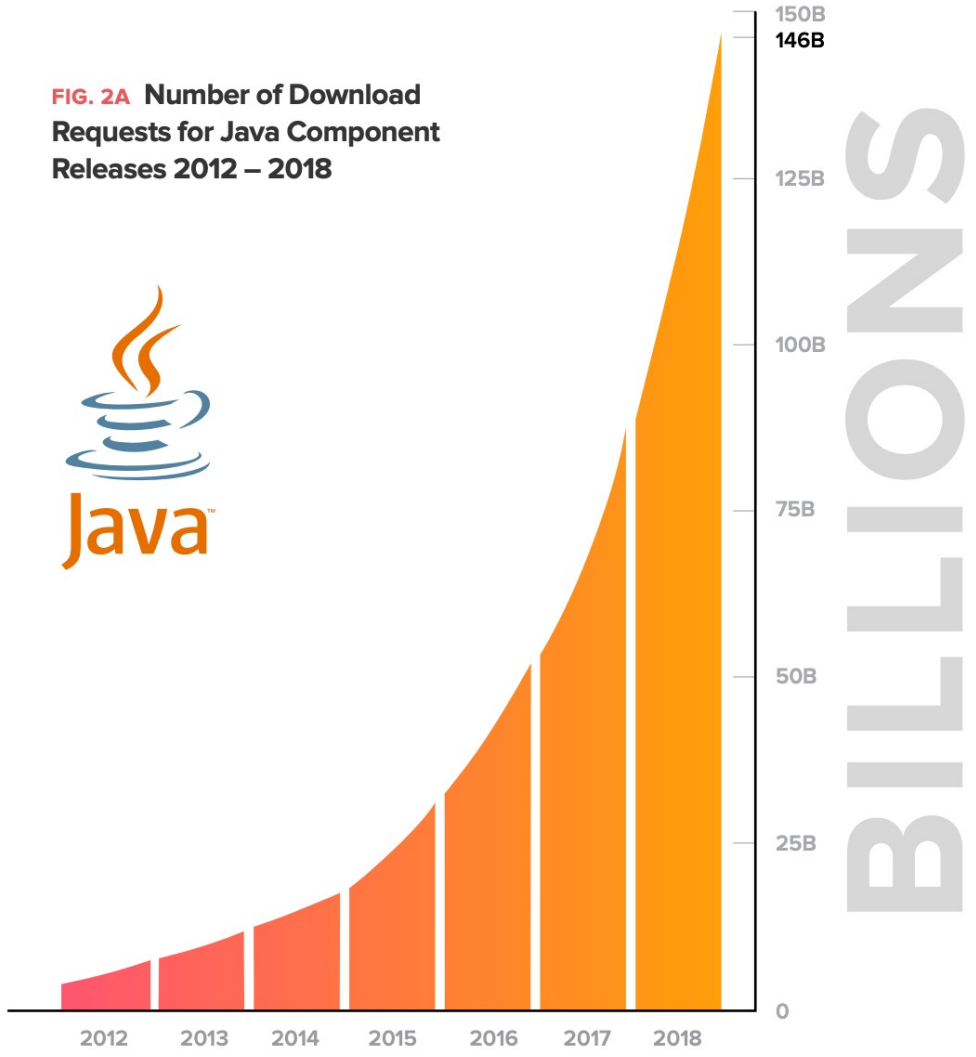
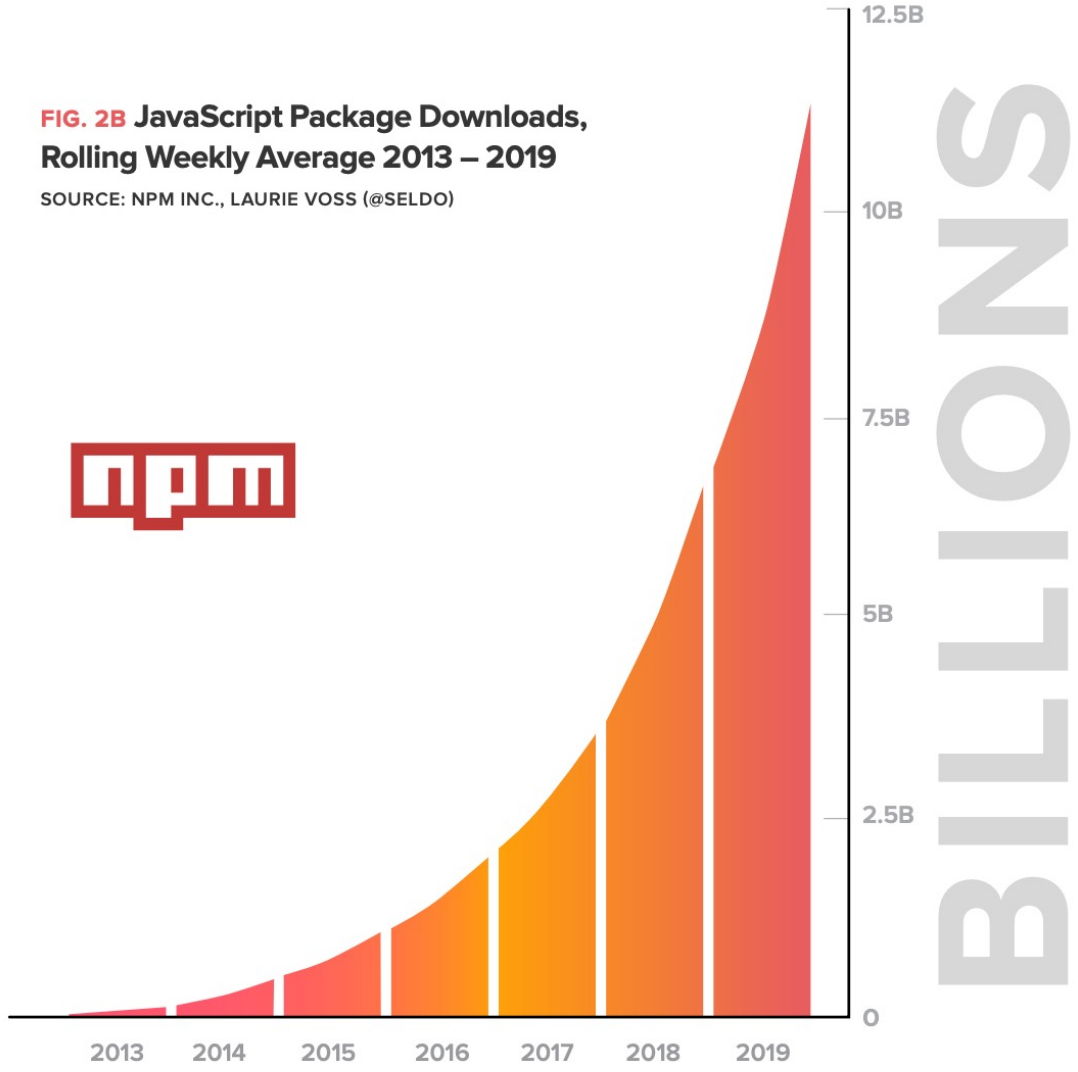


FIG. 2B **JavaScript Package Downloads, Rolling Weekly Average 2013 – 2019**

SOURCE: NPM INC., LAURIE VOSS (@SELDO)



OPTUM®

Vulnerability Incidents

Heartbleed Vulnerability

2014 - Security bug in the OpenSSL cryptography

Impacted **nearly 20% of secure web servers** on the Internet (almost half a million servers).

Allowed attackers to obtain access to **user passwords and session cookies**.

Theft of **4.5 million medical records** from a large hospital chain.

OPTUM®

Repackaging of Xcode for Malicious Code Distribution

2015 - “XcodeGhost”

39 applications available through the App Store were infecting iPhones and iPads.

Malicious applications connected to remote command-and-control servers and **uploaded sensitive user information** as part of a botnet.

Inserted into the applications through a **“repackaged” version** of Apple’s official development platform Xcode.

OPTUM®

“left-pad” Dependency Incident

2016 - Jenga tower of JavaScript

Dispute about naming rights caused a well-known developer to remove 273 packages from npm.

left-pad right-justifies text for more human-readable text output.

Relied upon by a number of critically important downstream packages - including Babel.

OPTUM®

Python Package (PyPI) Highjacking

2017, 2018

Malicious libraries with names that **“closely resembled”** the names of built-in Python libraries.

Installation script was changed to include malicious code.

Crytocurrency-stealing Python package called “Colourama”.

Legitimate package “Colorama,” one of the top-20 most-downloaded pieces of software within PyPI.

OPTUM®

Backdooring of “event-stream” Library

2018

Cryptocurrency-stealing code inserted into the package.

Malicious actors obtained legitimate publishing rights to the package itself by offering help to the beleaguered original developer.

Benign package, “flatmap-stream”, added to npm.

flatmap-stream added as a dependency to event-stream.

Malicious code added to flatmap-stream.

OPTUM®

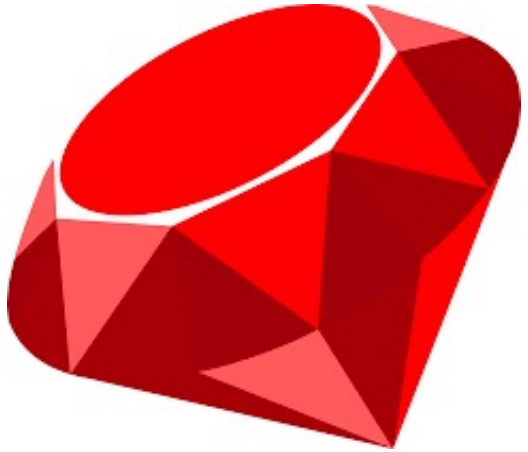
Account Takeover of Popular Ruby Gems Package

July 2019

strong_password, had been updated from 0.0.6 to 0.0.7, with code discrepancies b/w Github and Ruby repository.

Malicious code would contact a remote URL and retrieve additional code for remote code execution.

Ruby repository account had been taken over.



OPTUM®

Webmin Compromise

2018 - 2019

Webmin is a web-based interface for system administration for Unix.

Backdoor leveraging a specially-crafted URL to send commands to infected servers, which would then execute the commands with root privileges.

Server logs altered so that it looked like the file had not been updated in some time, hiding the change from common detection mechanisms like code comparison tools.

OPTUM®

Discovery of 11 Backdoored RubyGems Libraries

August 2019

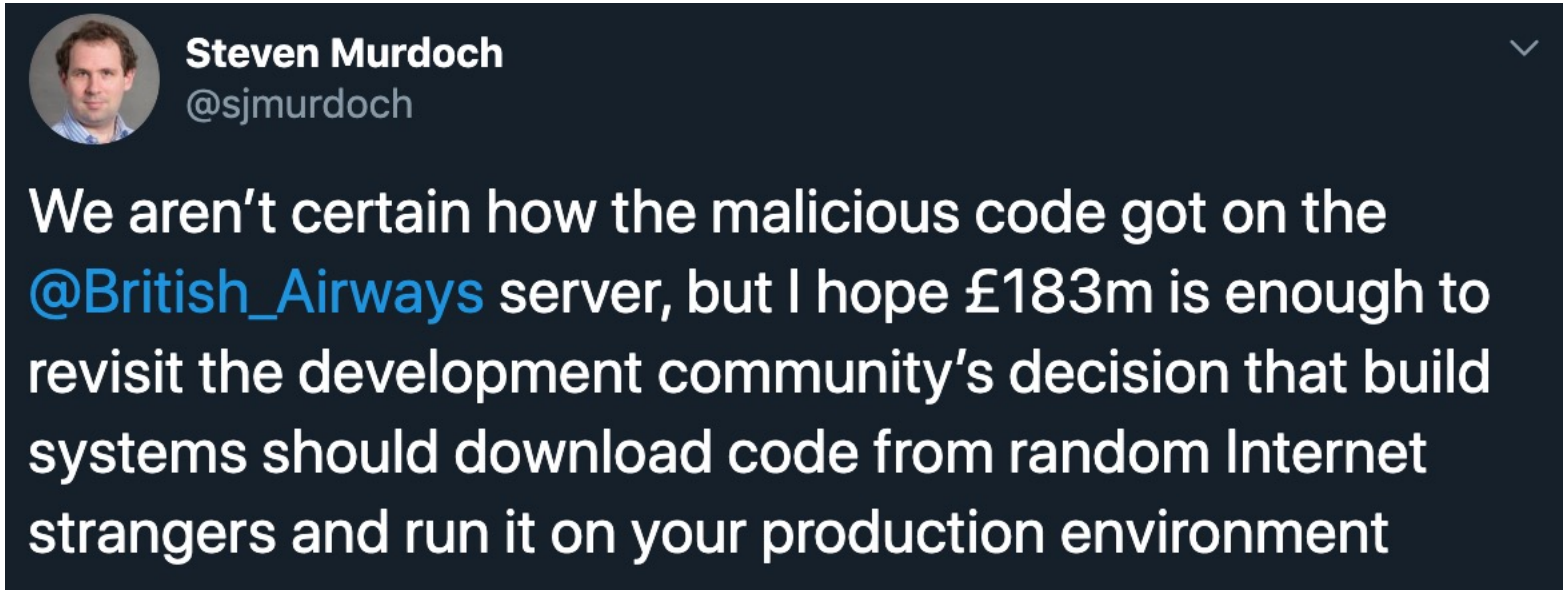
Allowed malicious actors in possession of pre-chosen credentials to remotely execute code on infected servers.

At least one of the packages infected due to the compromise of a developer account.

OPTUM®

British Airways fined $237M

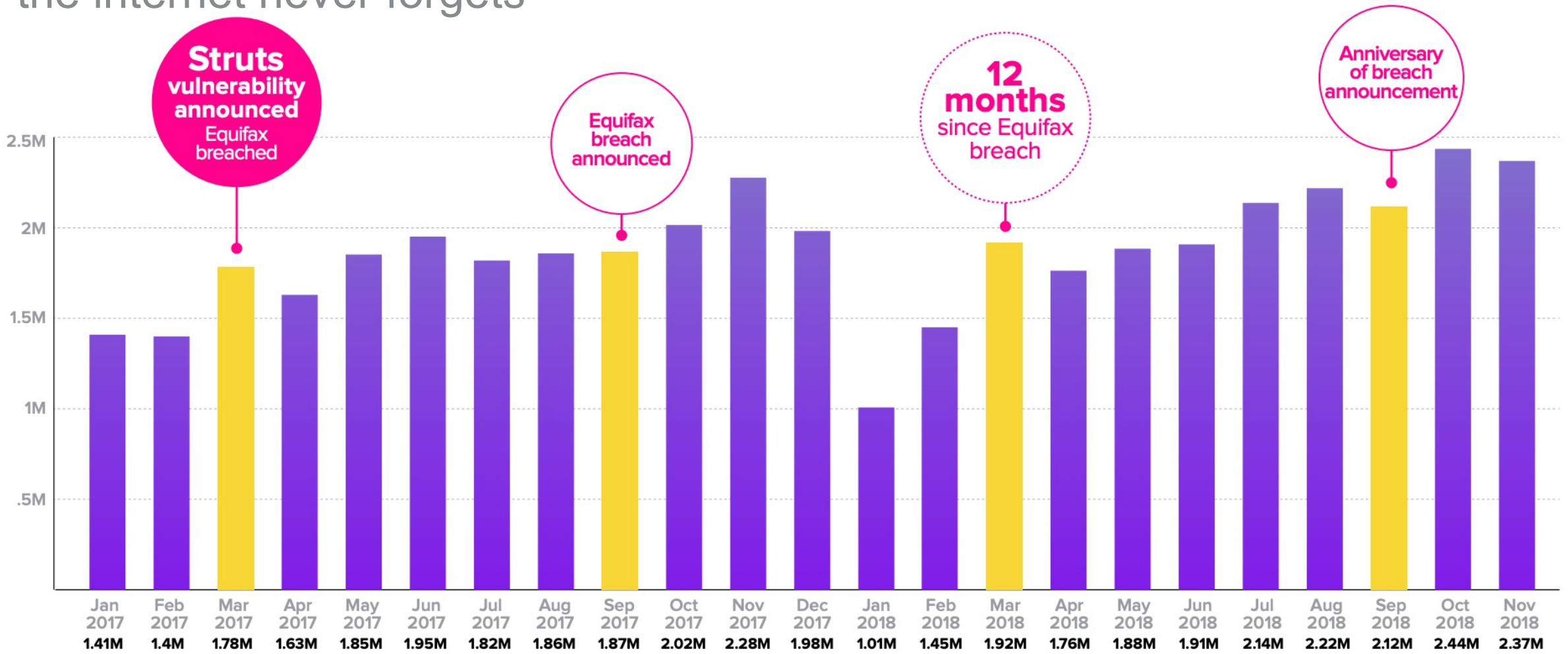
2019



OPTUM®

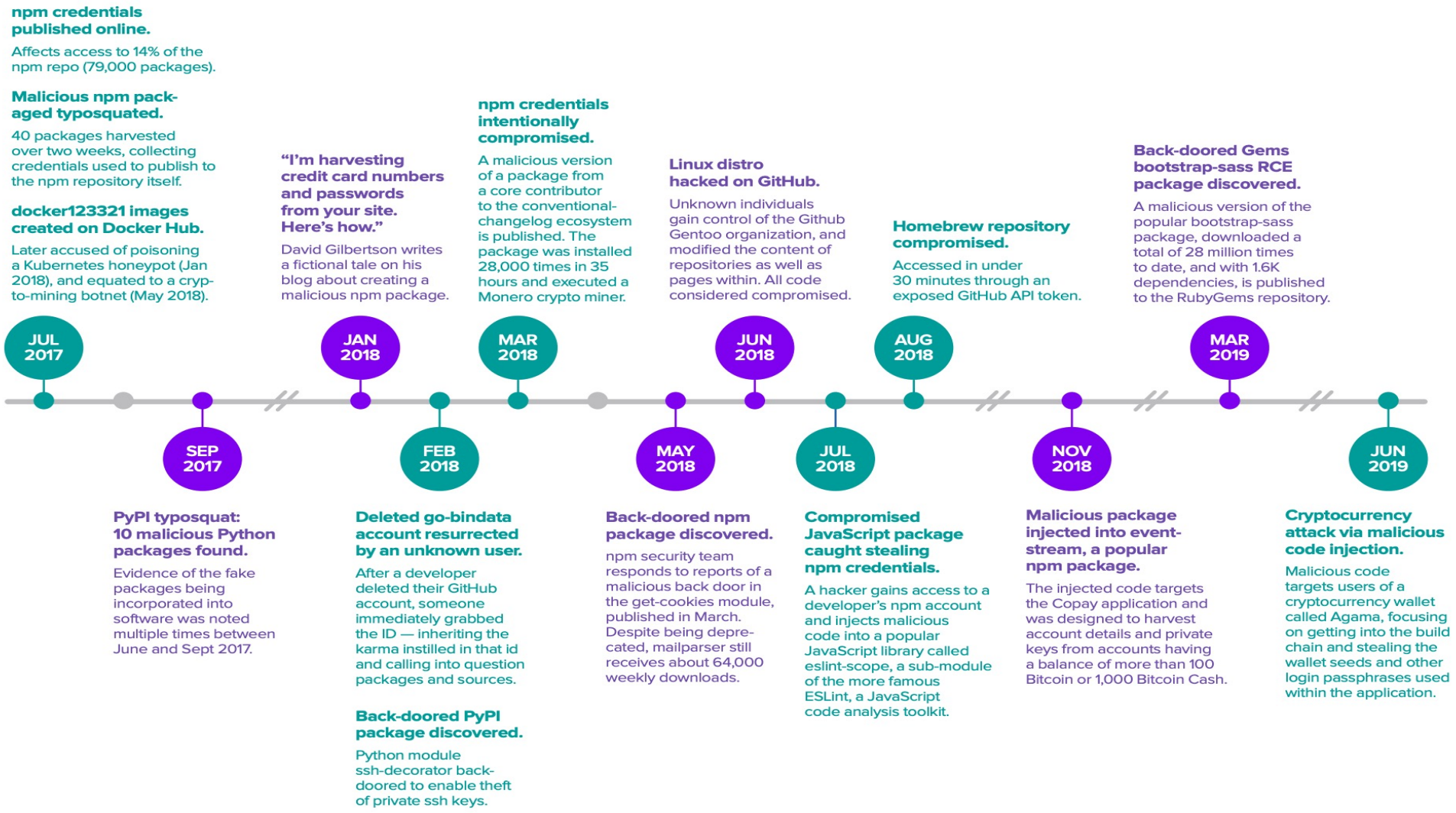
Post-Equifax

“the internet never forgets”



OPTUM®

Shifting Battlefront

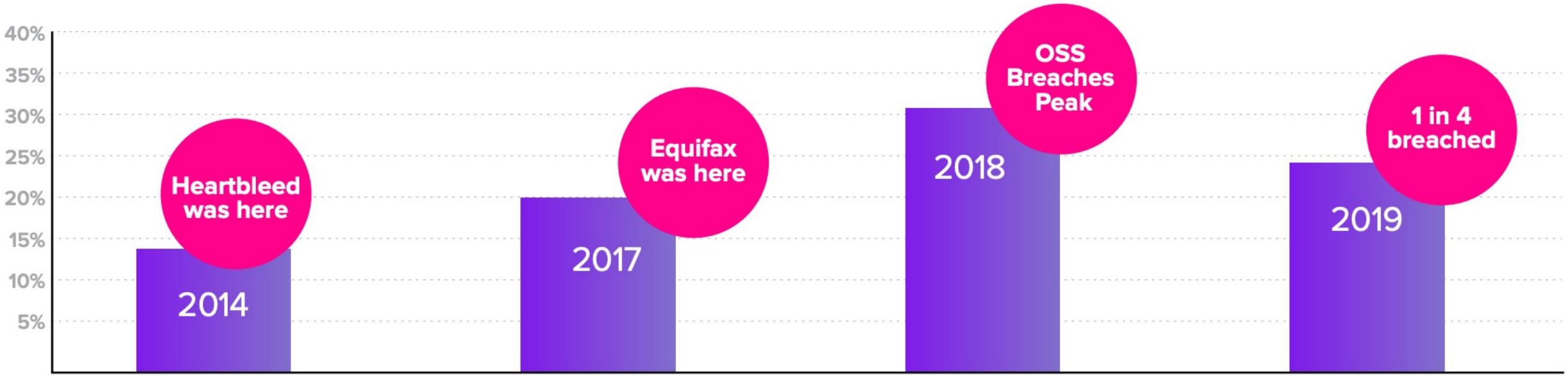


OPTUM®

Increasing attacks on Open Source

FIG 5C Suspected or Verified Open Source Related Breaches Over Four Years

SOURCE: DEVSECOPS COMMUNITY SURVEY (SONATYPE)



14%
suspect or have verified a breach related to open source components in the **2014 survey.**

20%
suspect or have verified a breach related to open source components in the **2017 survey.**

31%
suspect or have verified a breach related to open source components in the **2018 survey.**

24%
suspect or have verified a breach related to open source components **in the last 12 months.**

OPTUM®

Increasing attacks on Open Source

FIG 5A The Percentage of Vulnerable Java Components Downloaded Over Four Years

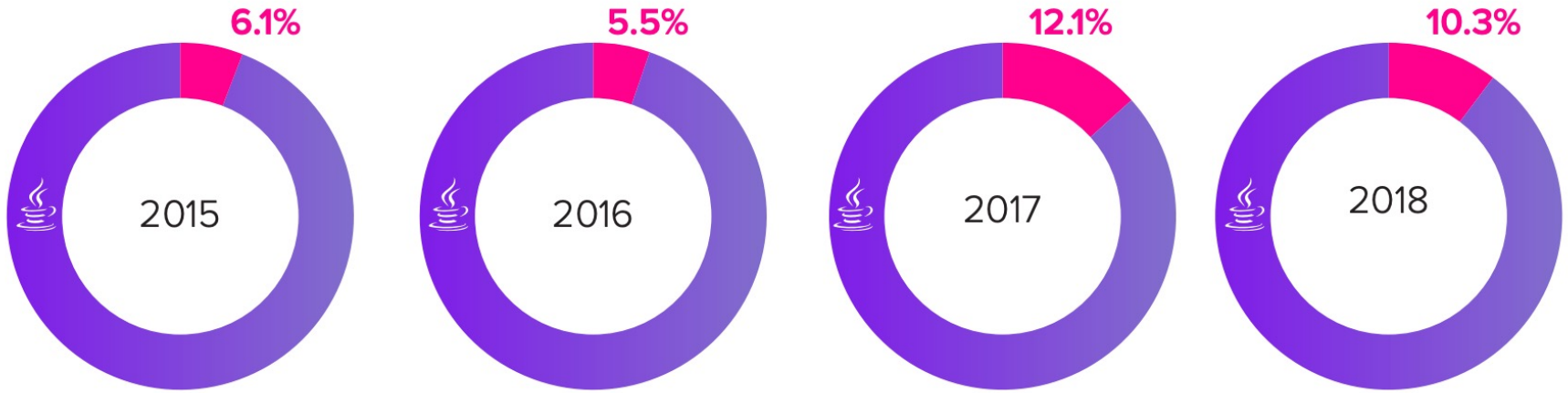
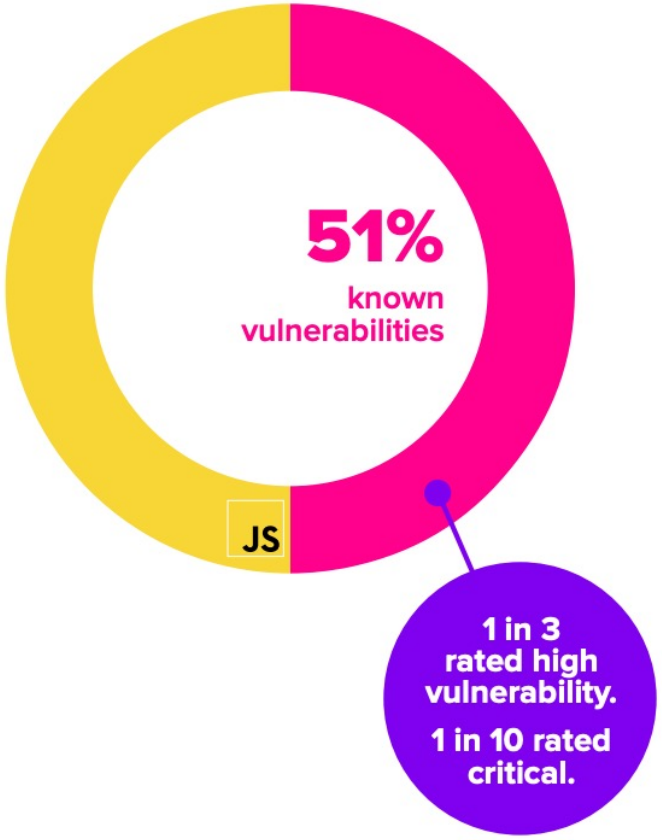


FIG 5B Half of JavaScript Package Downloads Contain Known Vulnerabilities

SOURCE: NPM QUICK AUDIT (4M SCANS PER WEEK)



OPTUM®

So, what's can be done?

OPTUM®

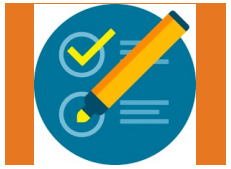
Developer Practices

Use 2FA/MFA for developer and other important accounts.

Require change control tracking throughout SDLC.

Use unique version identifier for each release.

Cryptographically sign or present verifiable proof of a project's integrity.

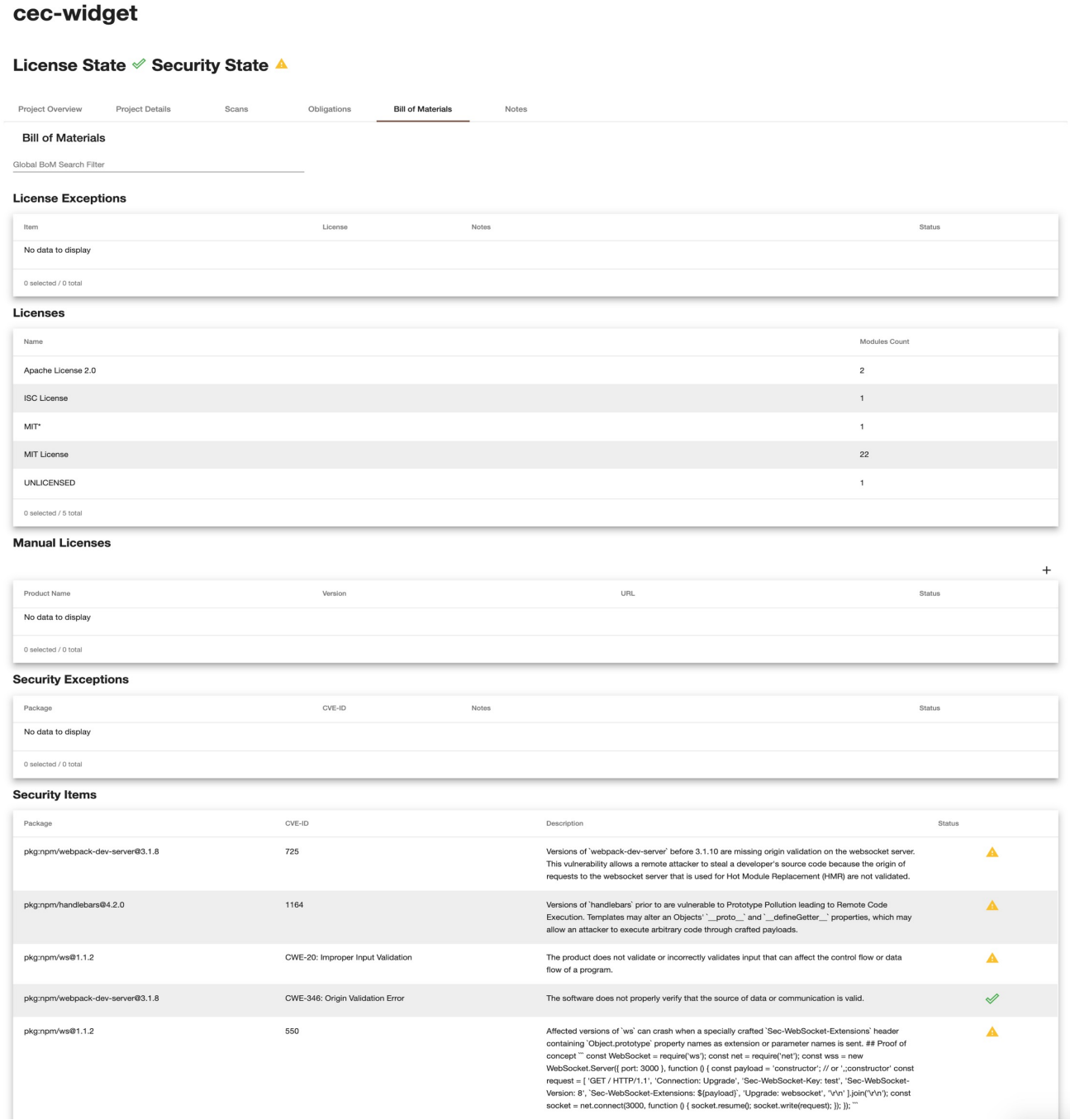


Integrate testing into SDLC to check common bugs, unexpected behavior, and malicious changes.

Leverage tools to track, analyze, and manage dependencies.

Document project dependencies in a way that is readily consumable by downstream users.

OPTUM®



Repositories

Language repositories lack basic security and quality controls

Few language repositories currently provides for a mechanism through which stored code is examined for its purpose.

Few language repositories perform systematic checks for vulnerabilities in stored code or for deprecated packages.

No language repository currently provides for a mechanism through which a consumer can tell if one piece of stored code is derived from another.

In most language repositories, weak or missing authentication and publisher verification mechanisms create uncertainty and risk over the provenance of stored code.

Some language repositories do not provide 2FA/MFA of developer accounts.

OPTUM®

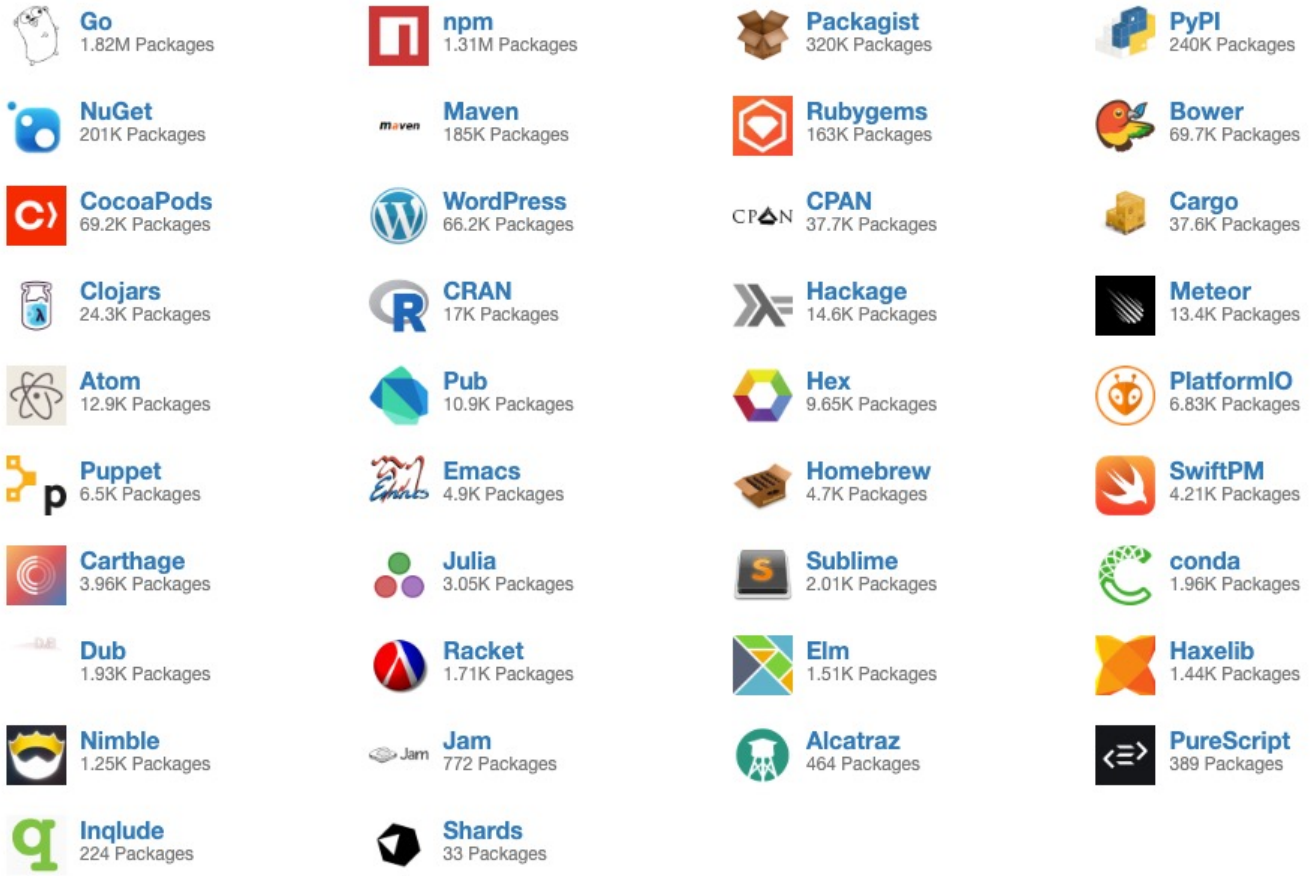
Project Dependency Managers

Package Managers

PDMs are simply software retrieval tools.

No checks on if retrieved software has known security or reliability issues.

No checks on if retrieved software contains unexpected or malicious behavior.



OPTUM®

Vulnerability Databases

Common Vulnerabilities and Exposures (CVE) & the National Vulnerability Database (NVD) programs

Missing or rejected vulnerabilities, leading to incomplete coverage in the NVD.

Severely delayed assignment of vulnerability identifiers, creating risks for downstream parties who remain unaware and likely unprotected from the issue.

Poorly contextualized descriptions of vulnerabilities, increasing the difficulty of mitigation and vulnerability management.

Overinflated and/or underplayed vulnerability scores, leading to misallocated resources and in some cases vulnerability “fatigue.”

Difficulty in revoking assigned vulnerabilities when they are found to be invalid, creating confusion and lack of trust in overall program.

OPTUM®

Vulnerability Databases

Social Issues with CVE and NVD

Abuse by developers who claim inflated numbers of vulnerabilities in order to pad resumes, creating “false positives.”

Abuse by engineers in organizations who see CVE assignments as a way to circumvent difficult management procedures preventing them from doing normal software upgrades.

Discomfort with the CVE program because it is managed by a US federal agency.

OPTUM®

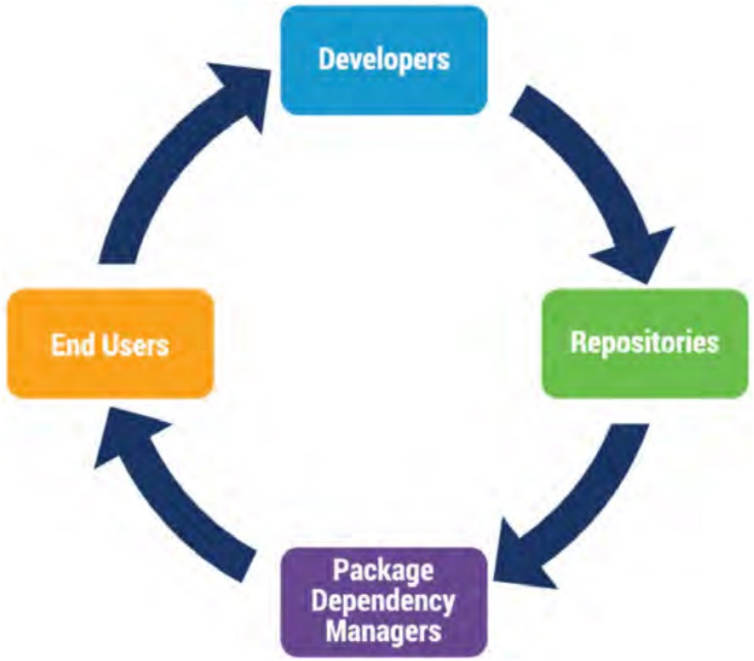
End User Practices

Define and control acquisition requirements

Require that dependency lists, software bills-of-material, or other such component tracking mechanisms are provided in a robust and transparent way.

Vulnerabilities within products maintained by a technology provider that are judged to have specific impacts must be remediated within certain timeframes.

Developers must use 2FA or MFA with any accounts related to the development of the software being acquired.



OPTUM®

Government and Industry Standards

What software components are being used, and how well they are supported?

Government and Industry Standards

U.S. Food and Drug Administration

Cybersecurity Bill of Materials (CBOM) for medical devices.

“to effectively manage assets, to understand the potential impact of identified vulnerabilities to the device, and to deploy countermeasures to maintain the device’s essential performance.”

MDMs may be subject to legal liabilities tied to the distribution of a medical device with a known vulnerability.

OPTUM®

Government and Industry Standards

U.S. House Energy and Commerce Committee

Cybersecurity Strategy Report details importance and priority for SBOM.

Permits risk decisions about which tech to purchase/use based on known vulnerability info.

Allows for quick identification & response to new vulnerabilities.

Minimizes the number of unknown unknowns.

OPTUM®

Government and Industry Standards

Payment Card Industry Security Standards Council

360 degree monitoring of open source component releases through SDLC.

Up to date inventory of open-source component releases utilized in software.

Process for identifying known vulnerabilities within open source component releases.

Policy and process to immediately remediate vulnerabilities as they become known.

OPTUM®

Government and Industry Standards

National Telecommunications and Information Administration (NTIA)

Requiring companies to list sources of software parts to protect U.S. software supply chains.

Focus on “Software Component Transparency” across manufacturers and vendors.

Defining standards around SBOM.

OPTUM®

Community Efforts

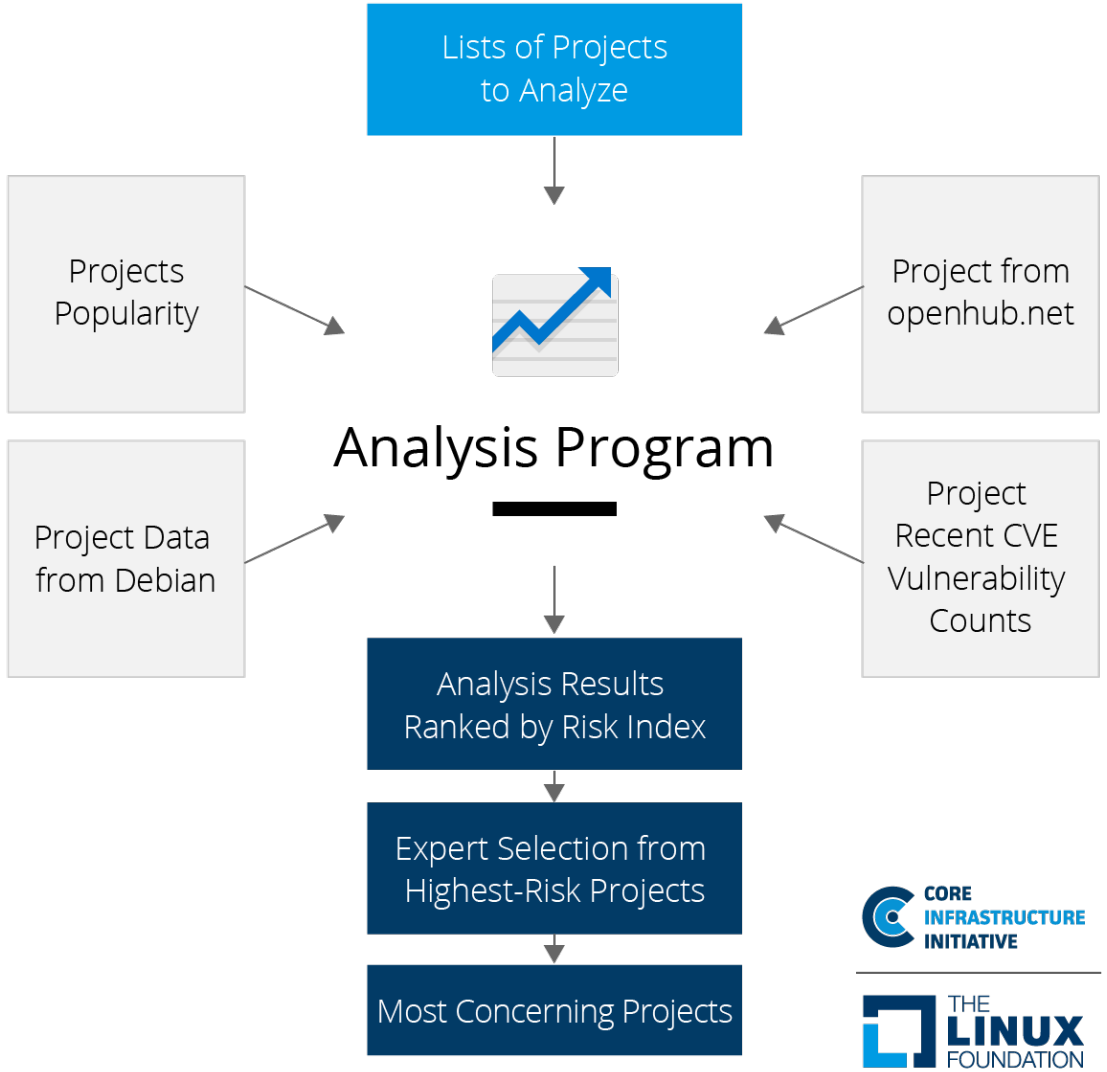
What software components are being used, and how well they are supported?

Linux Foundation - Core Infrastructure Initiative (CII)

Census Project ("Census I")

Identify which software packages in the **Debian Linux** distribution were the most critical to the kernel's operation and security.

Did not delve deeply into what software was deployed in production applications.



CORE INFRASTRUCTURE INITIATIVE

THE LINUX FOUNDATION

OPTUM®

Linux Foundation - Core Infrastructure Initiative (CII)

Census II

Identify the most commonly used free and open source software components in production applications.

Examine for potential vulnerabilities in these projects due to:

- Widespread use of outdated versions
- Understaffed projects
- Known security vulnerabilities

Prioritize investments/resources to support the security and health of FOSS.

OPTUM®

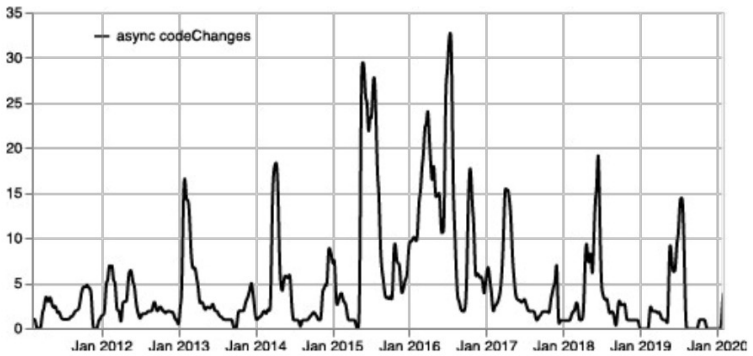
Linux Foundation - Core Infrastructure Initiative (CII)

async

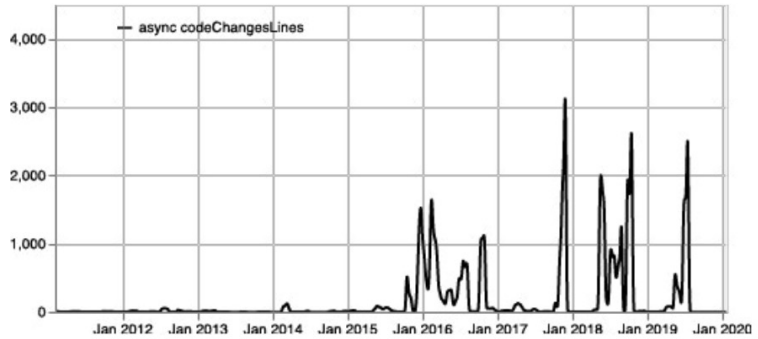
A utility module which provides straight-forward, powerful functions for working with asynchronous JavaScript. Although originally designed for use with Node.js and installable via npm install async, it can also be used directly in the browser.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/caolan/async	196,700 Lines	Authors: 22 Commiters: 7	86 total 1.65/week
As of February 7, 2020, this project has 11 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

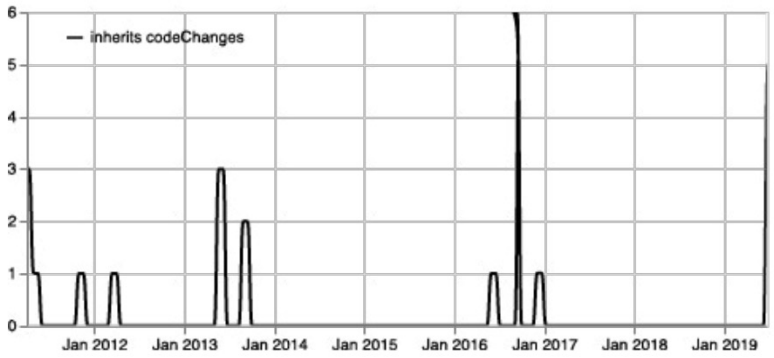
Linux Foundation - Core Infrastructure Initiative (CII)

inherits

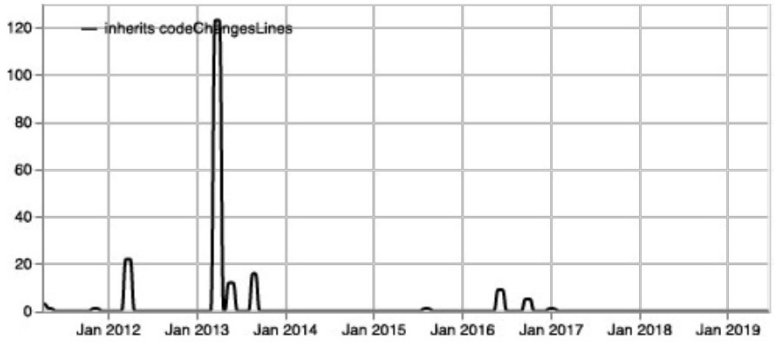
Browser-friendly inheritance fully compatible with standard node.js inherits.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/isaacs/inherits	3,800 Lines	Authors: 3 Commiters: 1	Gap, no commits between December 15, 2016 and June 19, 2019
As of February 7, 2020, this project has 3 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

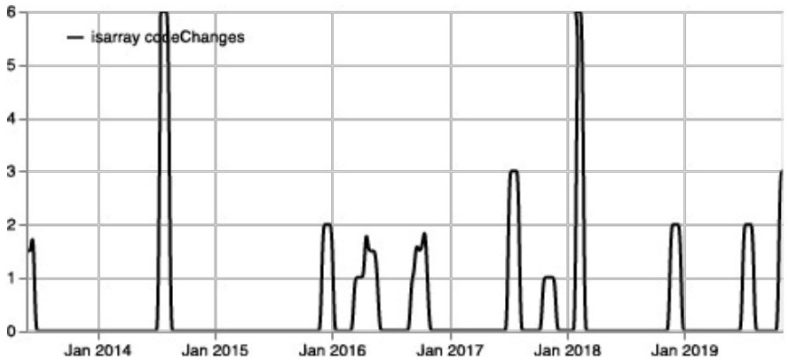
Linux Foundation - Core Infrastructure Initiative (CII)

isarray

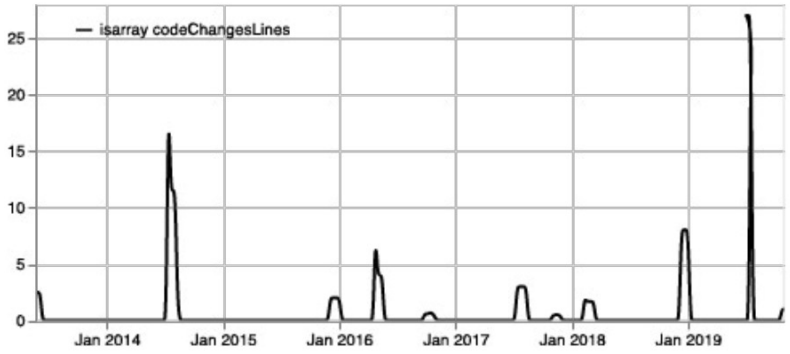
Array#isArray for older browsers and deprecated Node.js versions.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/juliangruber/isarray	317 Lines	Authors: 3 Commiters: 3	8 total 0.15/week
As of February 7, 2020, this project has 4 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

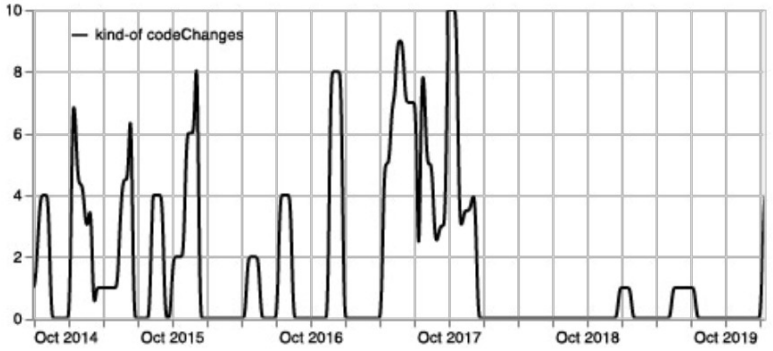
Linux Foundation - Core Infrastructure Initiative (CII)

kind-of

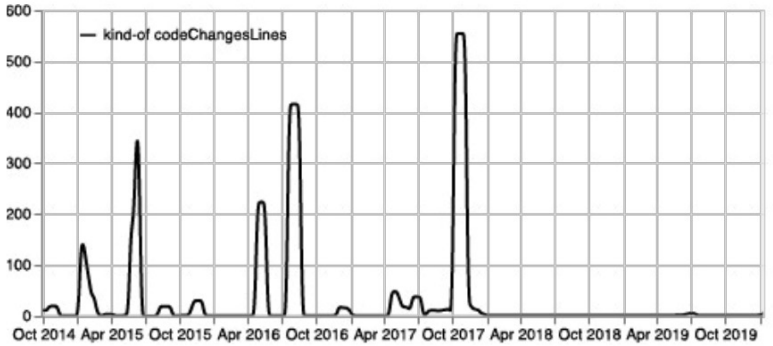
Get the native JavaScript type of a value.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/jonschlinkert/kind-of	2,000 Lines	Authors: 11 Commiters: 11	Gap, no commits between 2017-12-01 and 2019-05-25
As of February 7, 2020, this project has 3 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

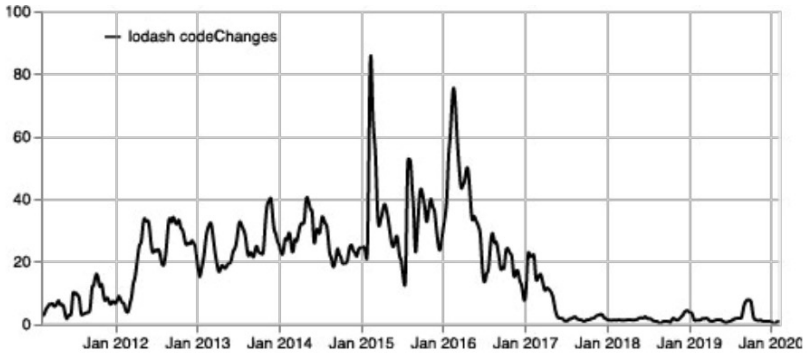
Linux Foundation - Core Infrastructure Initiative (CII)

lodash

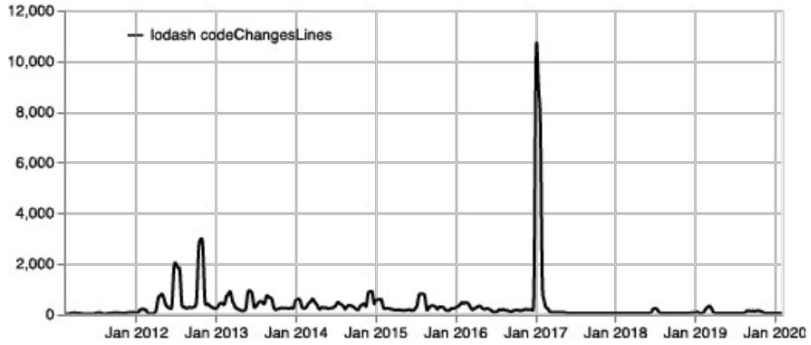
A modern JavaScript utility library delivering modularity, performance & extras.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/lodash/lodash	42,300 Lines	Authors: 28 Commiters: 2	58 total 1.12/week
As of February 7, 2020, this project has 30 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

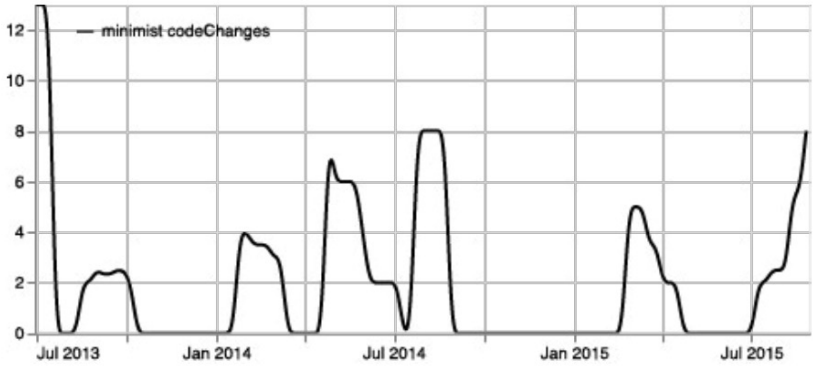
Linux Foundation - Core Infrastructure Initiative (CII)

minimist

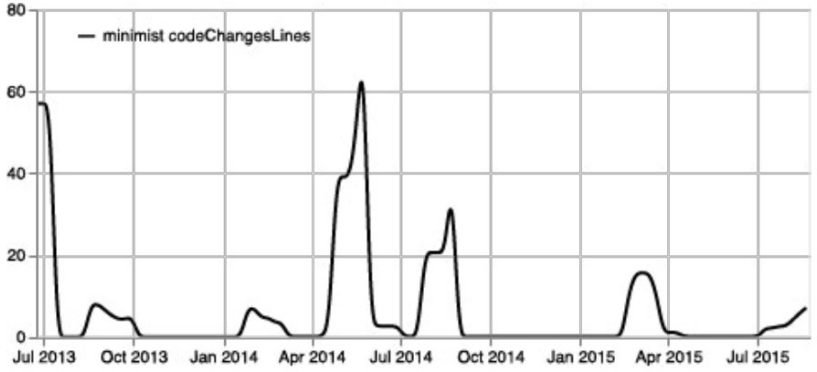
Parse argument options. This module is the guts of optimist's argument parser without all the fanciful decoration.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/substack/minimist	1,200 Lines	Authors: 14 Commiters: 6	Last commit: August 29, 2015
As of February 7, 2020, this project has 38 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

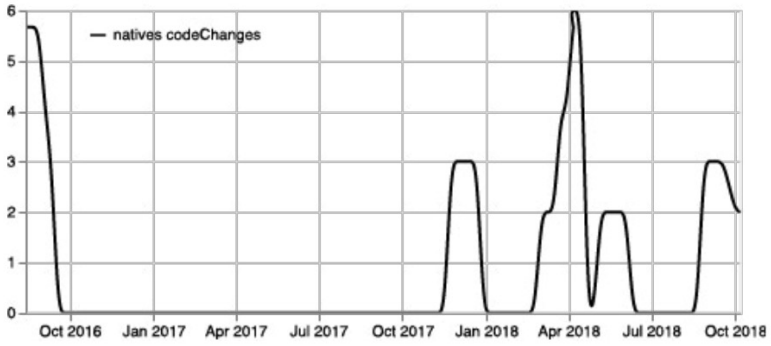
Linux Foundation - Core Infrastructure Initiative (CII)

natives

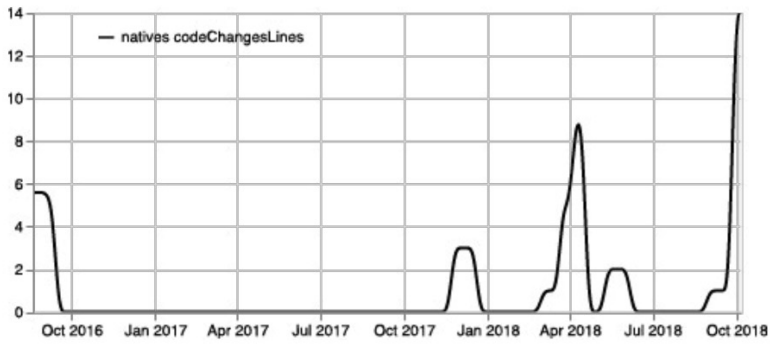
Do stuff with Node.js's native JavaScript modules.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/addaleax/natives	3,000 Lines	Authors: 2 Commiters: 1	15 total 0.29/week Last commit: October 8, 2018
As of February 7, 2020, this project has 0 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

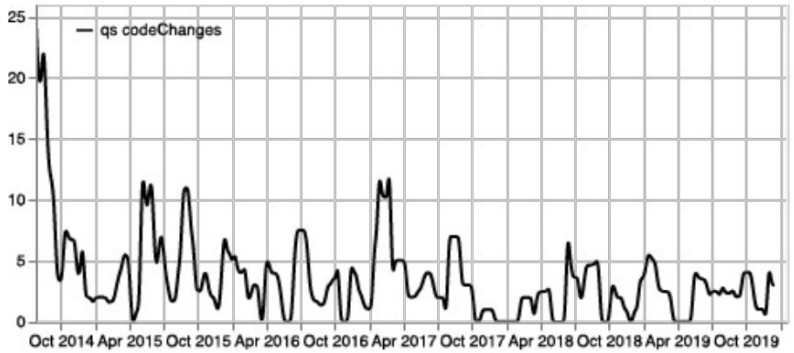
Linux Foundation - Core Infrastructure Initiative (CII)

qs

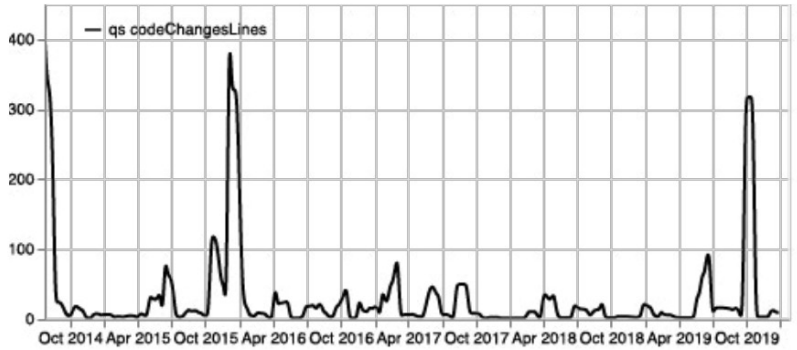
A querystring parsing and stringifying library with some added security.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/ljharb/qs	5,400 Lines	Authors: 5 Commiters: 2	36 total 0.69/week
As of February 7, 2020, this project has 41 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

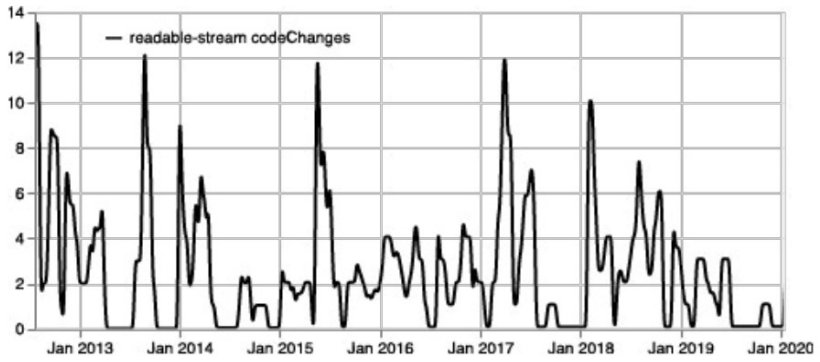
Linux Foundation - Core Infrastructure Initiative (CII)

readable-stream

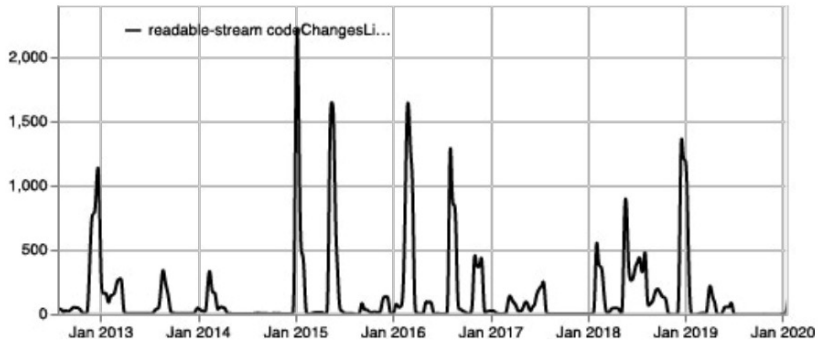
Node.js core streams for userland.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/nodejs/readable-stream	28,100 Lines	Authors: 10 Commiters: 3	69 total 1.33/week
As of February 7, 2020, this project has 21 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

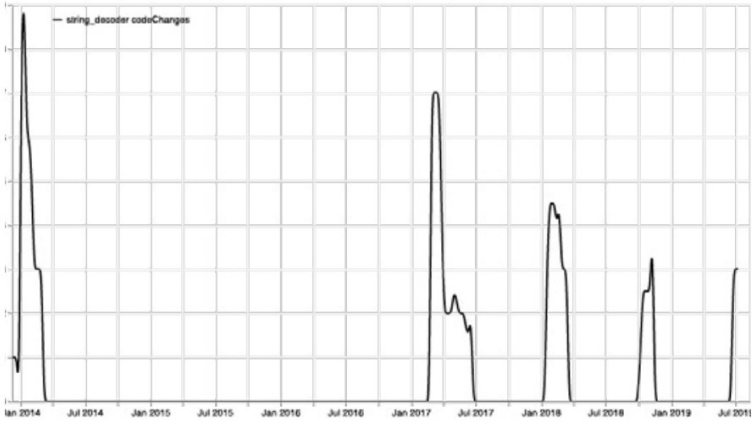
Linux Foundation - Core Infrastructure Initiative (CII)

string_decoder

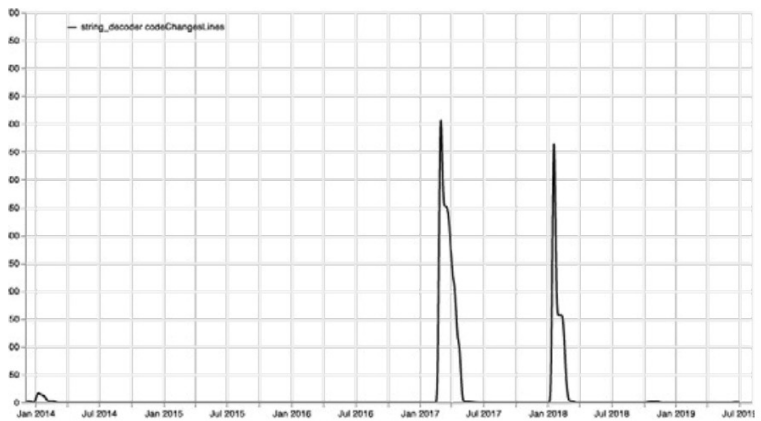
Node-core string_decoder for userland.

Platform	GitHub	Total Lines of Code	Active Contributors 2018	Commits 2018
npm	github.com/nodejs/string_decoder	4,200 Lines	Authors: 4 Commiters: 3	17 total 0.32/week
As of February 7, 2020, this project has 3 open issues on GitHub.				

Code Changes (Commits)/Week



Lines of Code Added/Week



OPTUM®

Linux Foundation - Core Infrastructure Initiative (CII)

Preliminary Findings

High correlation b/w being employed and being a top contributor.

2017 GitHub data found that some of the most active FOSS developers contributed to projects under their **Microsoft, Google, IBM, or Intel** employee email addresses.

The need for standardized naming schema for software components, for software supply chain transparency and security efforts.

7/10 of most used software packages are hosted under individual developer accounts.

The persistence of legacy software in Open Source.

ie: “yargs” vs “minimist”

OPTUM®

Linux Foundation - Core Infrastructure Initiative (CII)

Best Practices Badge Program

Document how to install and run (securely), and any API.

Have a distributed public version control system, including changes between releases.

Respond to bug reports within 14 days, and fix vulnerabilities.

Have an automated test suite that covers most of the code/functionality, and officially require new tests for new code.

Support HTTPS on the project sites.

OPTUM®

2973 Projects

Badge status All | Exclude passing | Text search Name or description text | Text search

Add New Project

Id	Name	Description	Website	License	Owner	Last achieved at	Tiered %	Badge
1	BadgeApp	BadgeApp is the web application that allows developers to provide information about their project and (hopefully) get a Core Infrastructure Initiative (CII)...	https://github.com/coreinfrastructure/best-practices-badge	MIT	David A. Wheeler	2016-01-12 22:55:00	300%	cii best practices gold
24	OWASP Zed Attack Proxy (ZAP)	OWASP Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be...	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	Apache-2.0	Simon Bennetts	2016-08-10 07:03:00	129%	cii best practices passing
26	TrouSerS	A software stack that provides a programmatic API to the computer's Trusted Platform Module (TPM) as specified by the Trusted Computing Group (TCG).	http://trousers.sourceforge.net	CPL-1.0	Charlemange		85%	cii best practices in progress 85%
29	Node.js	Node.js® is a JavaScript runtime built on Chrome's V8 JavaScript engine	https://nodejs.org	MIT	Rod Vagg	2016-02-12 01:57:00	107%	cii best practices passing
31	OSSEC	OSSEC is an Open Source Host-based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection,...	http://ossec.github.io	GPL-2.0	Scott R. Shinn		98%	cii best practices in progress 98%
33	Ruby on Rails	Ruby on Rails is an open-source web framework that's optimized for programmer happiness and sustainable productivity. It favors convention over configuration.	http://rubyonrails.org	MIT	Dan Kohn		94%	cii best practices in progress 94%
34	Linux Kernel	The Linux kernel.	https://www.kernel.org	GPL-2.0	Greg Kroah-Hartman	2018-06-14 16:10:57	296%	cii best practices silver

OPTUM®

Linux Foundation - Trust and Security Initiative

Trust and Security Initiative

Eight Best Practices

Roles and Responsibilities

Security Policy

Know Your Contributors

The Software Supply Chain

Technical Security Guidance

Security Playbooks

Security Testing

Secure Releases and Updates

Certification Scheme

Based on Cloud Security Alliance or CSA STAR program models.

Other Security Issues

Security Build Certificate

Lack of good Open Source Security Testing Tools

Open Source Package Distribution is a Risk to the Internet

Vulnerability Disclosure is Broken

OPTUM®

Open Source Organizations

Choose Projects backed by reputable communities

Conclusion

Conclusion

Health and Security of FOSS Supply Chain

Global Demand for Open Source	Software Supply Chain	Challenges	Ongoing Efforts
The growing demand for innovation accelerating open source consumption.	Ensuring the **health and security of FOSS Supply Chain is critical** to the future of nearly all industries in the modern economy.	Increasing number of components Transitive dependencies Lack of security/quality controls across SSC	Government and Industry Standards The Linux Foundation Core Infrastructure Initiative Trust and Security Initiative

OPTUM®

References

Vulnerabilities in the Core: Preliminary Report and Census II of Open Source Software

2019 State of the Software Supply Chain

Open Source Software Supply Chain Security