

# Cover Your Apps While Still Using npm

Tierney Cyren

OCTOBER 23, 2018

NODESOURCE®

# \$ whoami

# NODESOURCE®

## DEVELOPER ADVOCATE



**Community Committee**

**Moderation Team**

**Website Redesign**

**Automation**

**Governance**

**Bootstrap**

@bitandbang



# npm: the numbers



815,000 packages

6,500,000,000 downloads last week

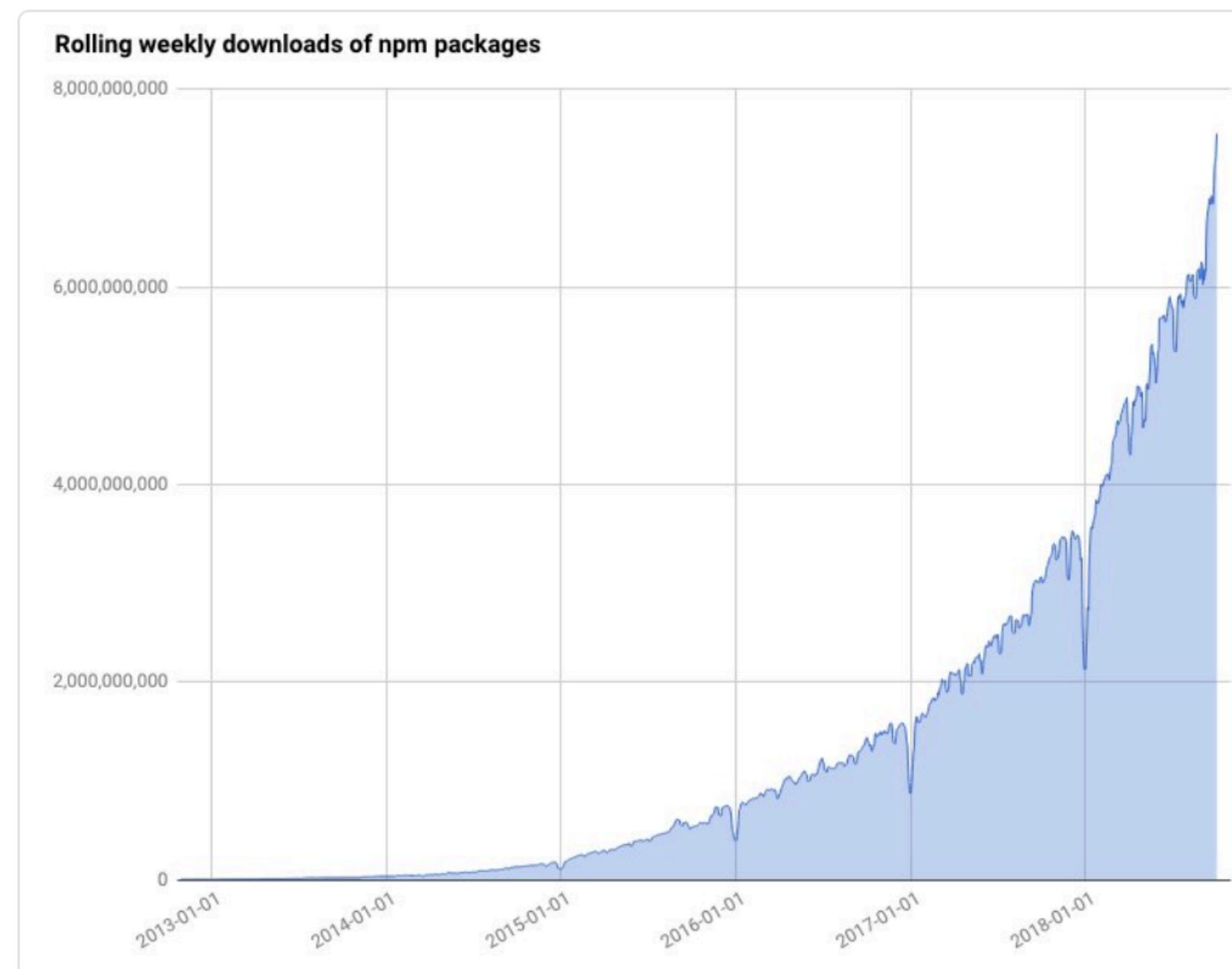
26,500,000,000 downloads last month



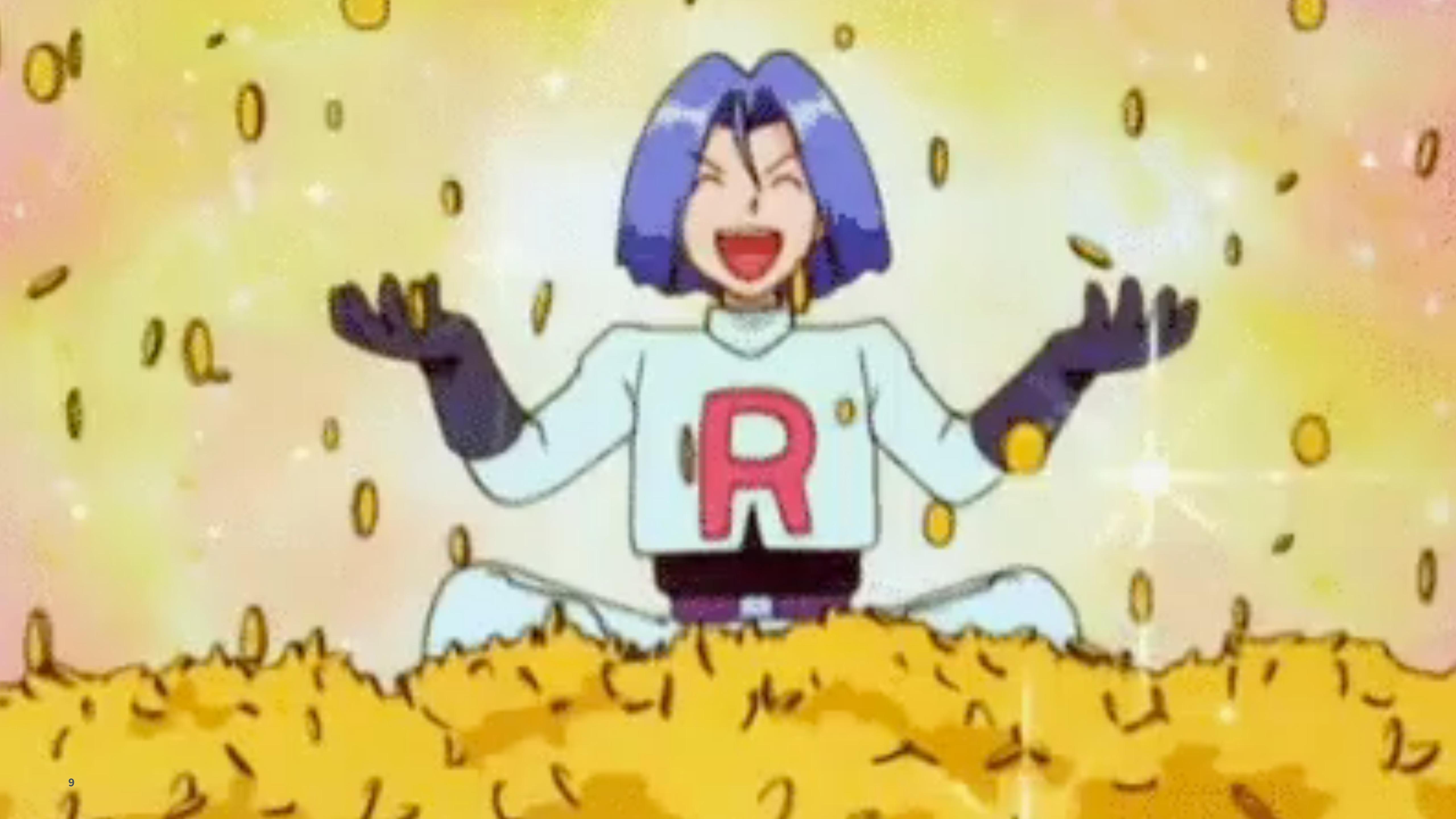
Laurie Voss  
@seldo

Following

September is always a strong month for npm Registry growth (you can see previous Septembers in this graph) and this one is no exception: npm users download 7.5 billion packages in the last 7 days.



8:19 PM - 3 Oct 2018



# We have a large and diverse ecosystem

- There's *probably* already a module to do what you want
- You can build out prototypes extremely quickly, and iterate from there
- There's a diverse set tools to solve your problems
- There's a large pool of talent – both junior and senior
- You only need to know JavaScript to do *anything* you want to



credit: [webcomicname.com](http://webcomicname.com) / [@dorismccomics](https://twitter.com/dorismccomics) / [npmjs.com](http://npmjs.com) / [@npmjs](https://twitter.com/npmjs)

# We have a large and diverse ecosystem

- There's *probably* multiple modules to do what you want
  - How do you choose?
  - How can you know you trust all the modules you're using?
    - Do you even **know** all the modules you're using?
  - What tools can you use to ensure you're shipping secure code?
  - What do you do when there's an outage?

# Software Repositories are Key Internet Infrastructure



How many of you trust GitHub?

A screenshot of a web browser window titled "GitHub System Status". The URL in the address bar is "https://status.github.com/messages". The page content is from GitHub's status page, showing a history of system messages. At the top right, it says "UPDATED ABOUT 14 HOURS AGO". Below that, a section titled "Status Messages" shows a list of messages. The first message is dated "October 22, 2018". Subsequent messages are listed with their respective times and descriptions.

**GitHub Status**

UPDATED ABOUT 14 HOURS AGO

**Status Messages**

October 22, 2018

14:26 Eastern We have resumed webhook delivery and will continue to monitor as we process  
Daylight Time the backlog of events.

14:09 Eastern Webhook delivery remains paused while we work through an issue. We are  
Daylight Time currently deploying a fix, and expect to resume delivery soon.

13:32 Eastern We have temporarily paused delivery of webhooks while we address an issue. We  
Daylight Time are working to resume delivery as soon as possible.

12:51 Eastern We have resumed Pages builds and will continue to monitor as we process a  
Daylight Time delayed backlog of events.

12:45 Eastern We have resumed delivery of webhooks and will continue to monitor as we  
Daylight Time process a delayed backlog of events.

12:24 Eastern We've completed validation of data consistency and have enabled some  
Daylight Time background jobs. We're continuing to monitor as the system recovers and expect  
to resume delivering webhooks at 16:45UTC.

11:09 Eastern Background jobs remain paused as we near completion of validation of data  
Daylight Time consistency.

09:18 Eastern We are validating the consistency of information across all data stores. Webhooks  
Daylight Time and Pages builds remain paused.

07:56 Eastern The majority of restore processes have completed. We anticipate all data stores  
Daylight Time will be fully consistent with the next hour.



How many of you trust npm?

The screenshot shows a web browser window for the npm Inc. Status page at <https://status.npmjs.org>. The page features the red npm logo at the top left. To its right is a blue "SUBSCRIBE TO UPDATES" button. A prominent green bar across the middle of the page displays the text "All Systems Operational". Below this, a section titled "About This Site" contains a message from npm stating: "npm loves you. Here is some info about how well it's doing. (You can also follow these updates at @npmstatus on Twitter!)" At the bottom of the page, there is a table showing uptime for various locations over the past 90 days. The table has two columns: "Registry Reads" and "Website Reads", each with four rows corresponding to US East (NYC), US East (IAD), US Central (DAL), and US East (ASH), US East (ATL), US Central (CHI). All entries show a green checkmark indicating uptime.

Registry Reads	Website Reads
US East (NYC)	✓
US East (IAD)	✓
US Central (DAL)	✓
US East (ASH)	✓
US East (ATL)	✓
US Central (CHI)	✓

Should you **trust** software  
repositories like npm to be perfect?





**malice ghoulpus**  
@alicegoldfuss

Following



Systems failure is guaranteed. Recovery  
isn't.

7:56 PM - 22 Oct 2018



really good at making software  
configurable & extensible

What can you do to  
cover your apps?

# Set up a Registry

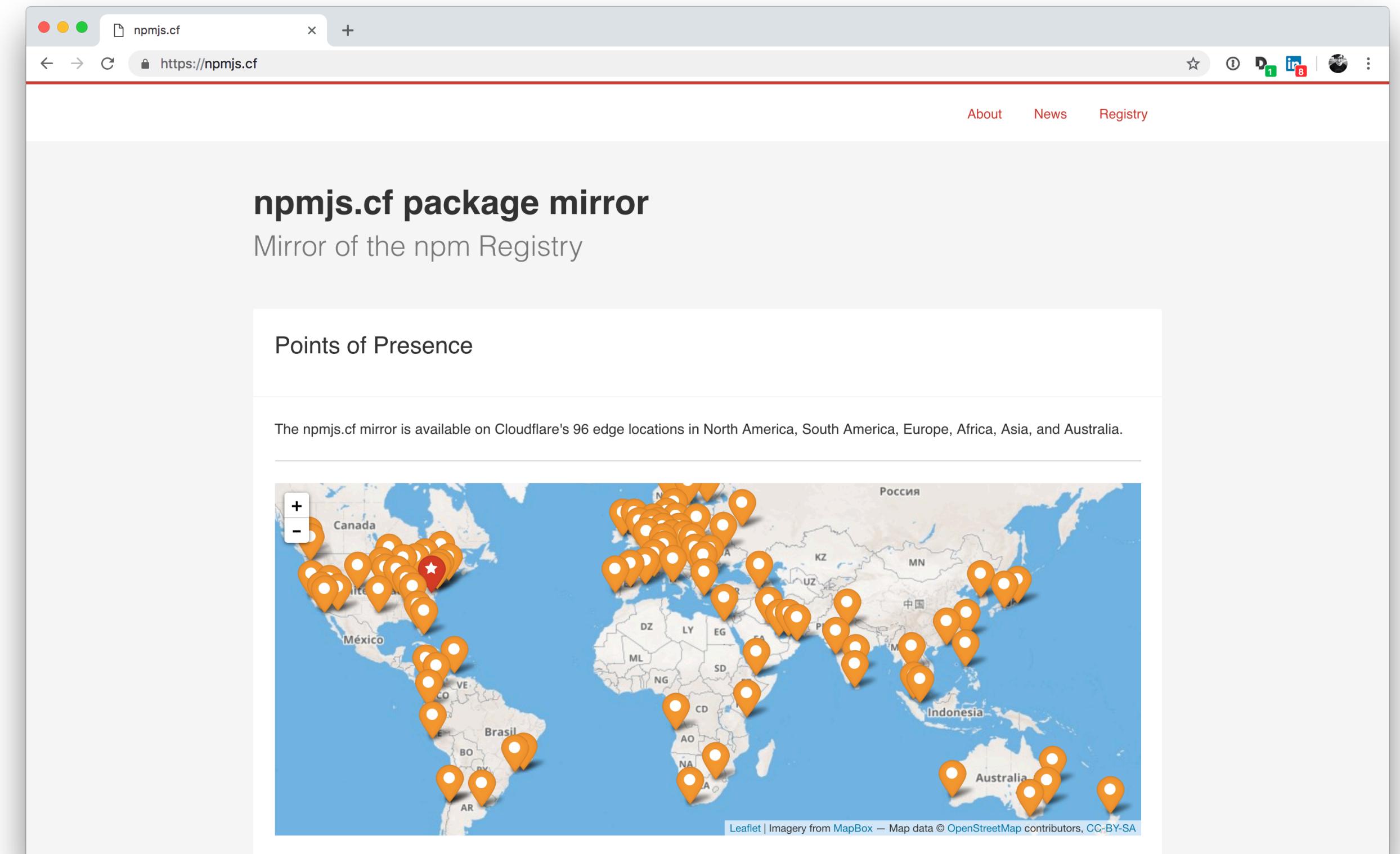
# Mirror as a Fallback

[npmjs.cf](https://npmjs.cf) / [cnpmjs.org](https://cnpmjs.org) / roll your own

# Set up a Registry Mirror as a Fallback

npmjs.cf

npm registry mirror on CloudFlare,  
maintained by a CloudFlare employee.



# Set up a Registry Mirror as a Fallback

cnpmjs.org

Chinese mirror of the npm registry, originally used by JavaScript developers in China as a solution for ensuring there aren't issues between the Great Firewall and npmjs.com.

The screenshot shows a web browser window displaying the cnpmjs.org homepage. The title bar reads "cnpmj.org: Private npm registry" and the URL is "https://cnpmj.org". The page features a large blue "CNPM" logo at the top left. To its right is a banner for "Alibaba Cloud" with the text "高性能云服务器首台5折" and a "立即选购" button. A search bar labeled "Search Packages" is positioned on the right side of the banner. Below the banner, the text "cnpmj.org: Private npm registry and web for Company" is displayed in bold. A subtext explains that "cnpm" means "Company npm". A section titled "Registry" lists the following information:

- Our public registry: [r.cnpmj.org](https://r.cnpmj.org), syncing from [registry.npmjs.com](https://registry.npmjs.com)
- cnpmj.org version: 3.0.0-rc.6
- Node.js version: v10.9.0
- For developers in China, please visit [the China mirror](#). 中国用户请访问[国内镜像站点](#).

Below this, there are three data tables showing package statistics:

842,568	total packages	6,819,186	total package versions	98	total delete packages
678,397	downloads today	1,275,878	downloads in this week	10,349,066	downloads in this month
597,481	downloads in the last day	3,746,774	downloads in the last week	14,320,215	downloads in the last month

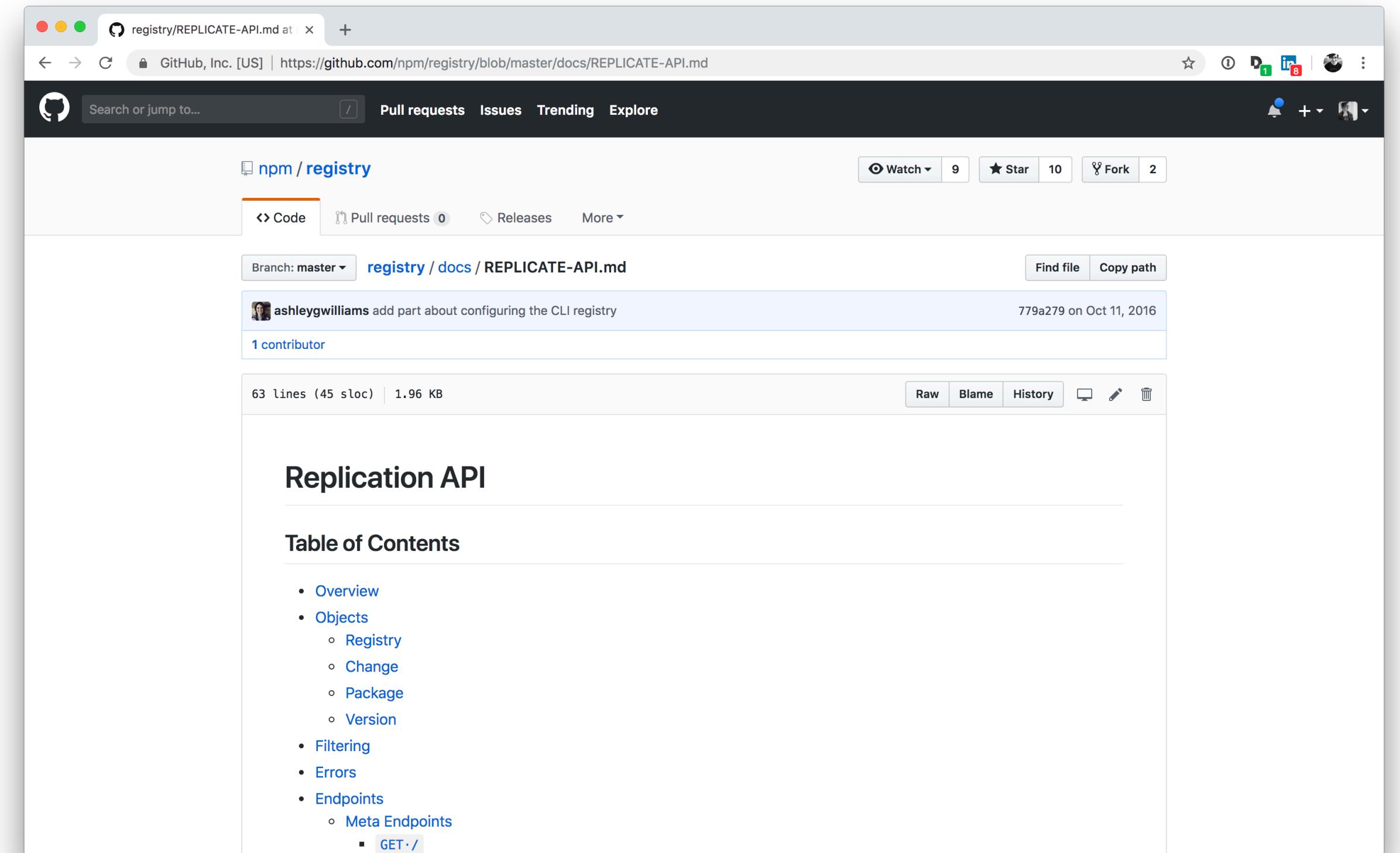
A "Sync Status" section indicates that the registry will sync all packages from the official registry, with the last sync time being "Thu Jun 22 2017 07:59:54 GMT-0400 (Eastern Daylight Time)". It also shows "1 packages need to be sync" and "0% progress".

# Set up a Registry Mirror as a Fallback

## Roll Your Own

You can prop up your own mirror to ensure you've got **maximum** uptime.

If you roll your own, why not make it public and ... the ❤?



[nsrc.io/replicate-guide](https://nsrc.io/replicate-guide)

# Cache Locally & Publish Privately

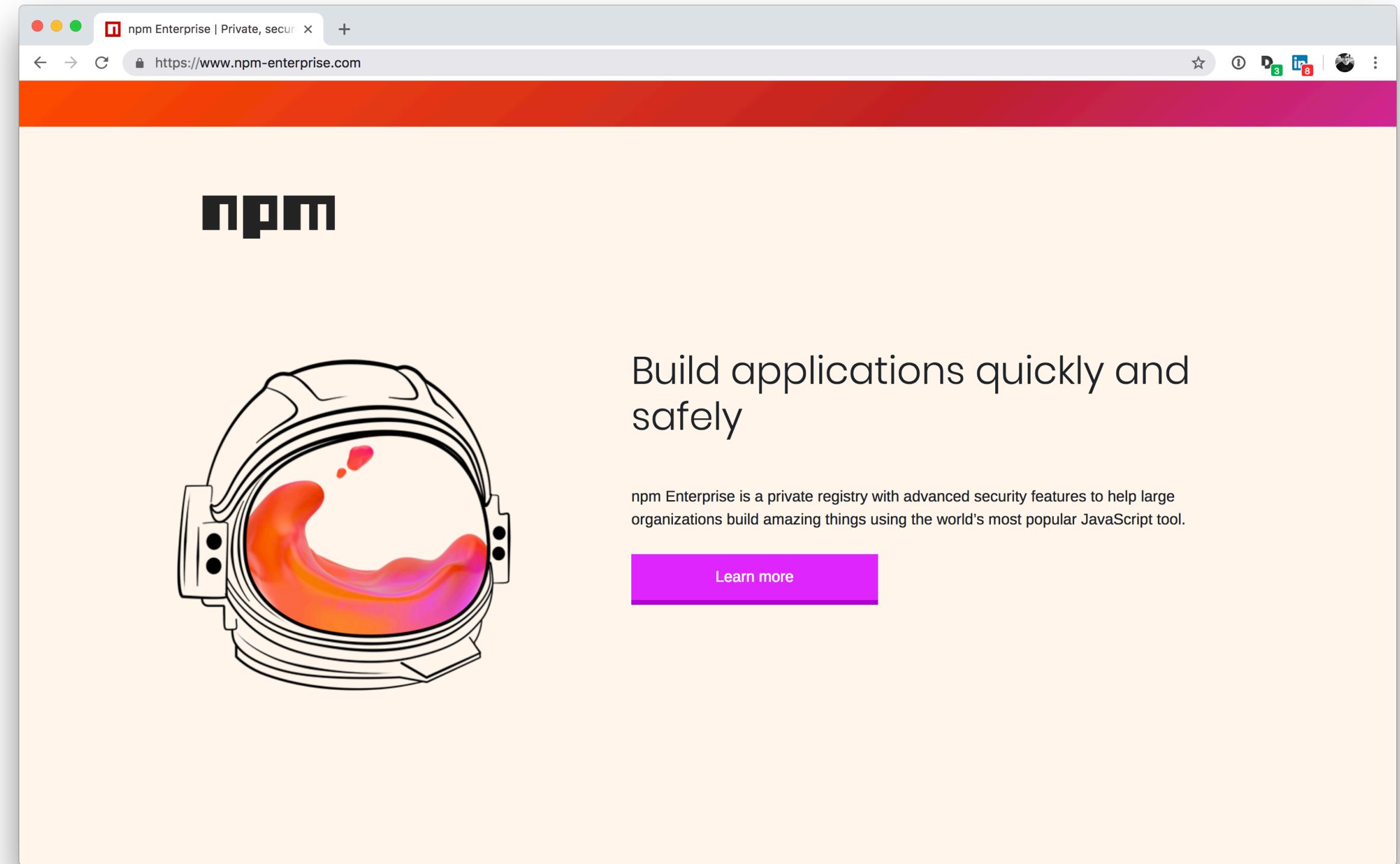
**Enterprises:** npm Enterprise / jFrog Artifactory

**Developers/DIY:** Verdaccio / Git / local-npm

Cache Locally & Publish Privately

# npm Enterprise

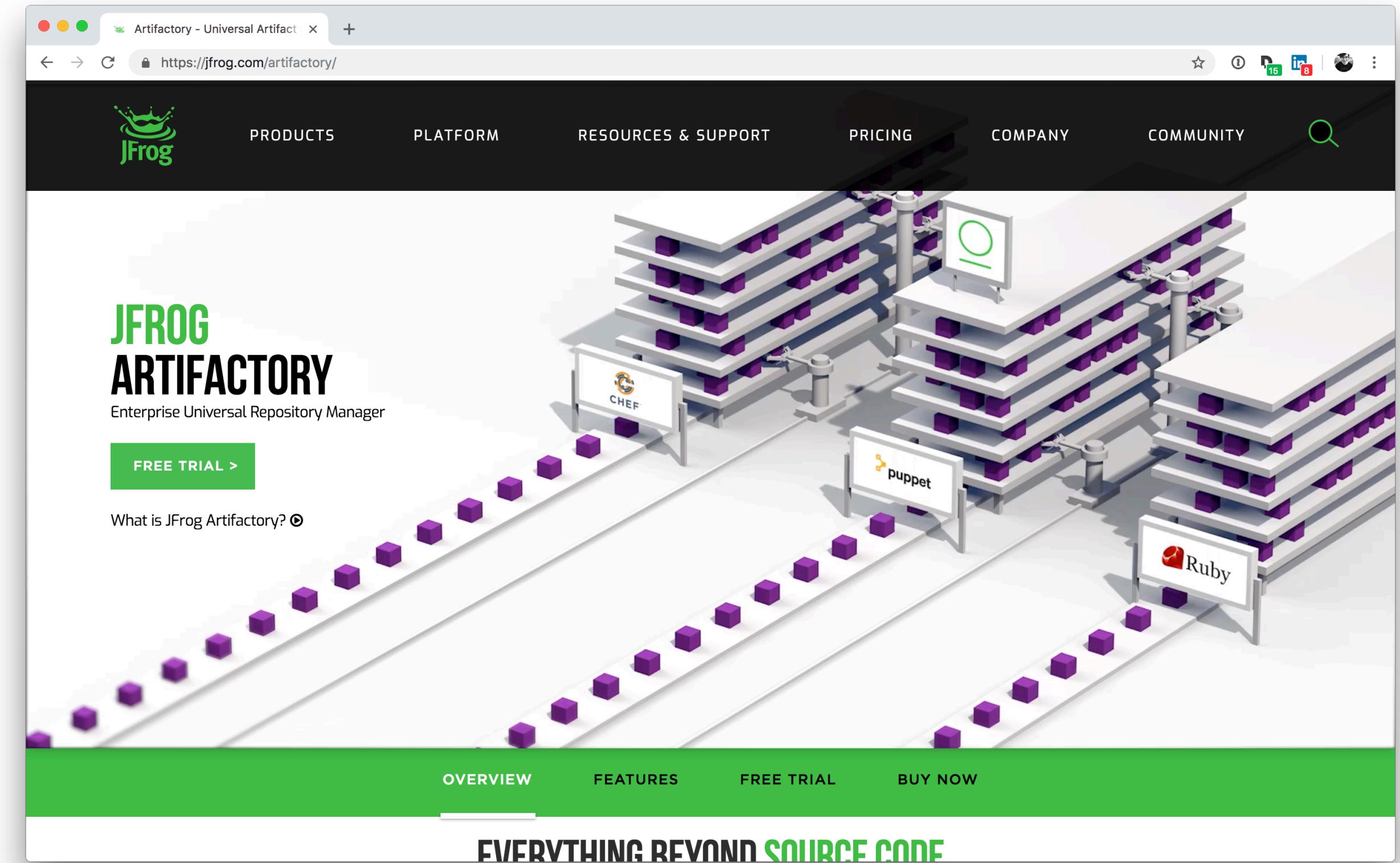
npm's own single tenant,  
enterprise-grade private registry  
on GKE.



# Cache Locally & Publish Privately

## jFrog Artifactory

jFrog's solution to a private registry. If you already have Artifactory, this is a quick and easy win.



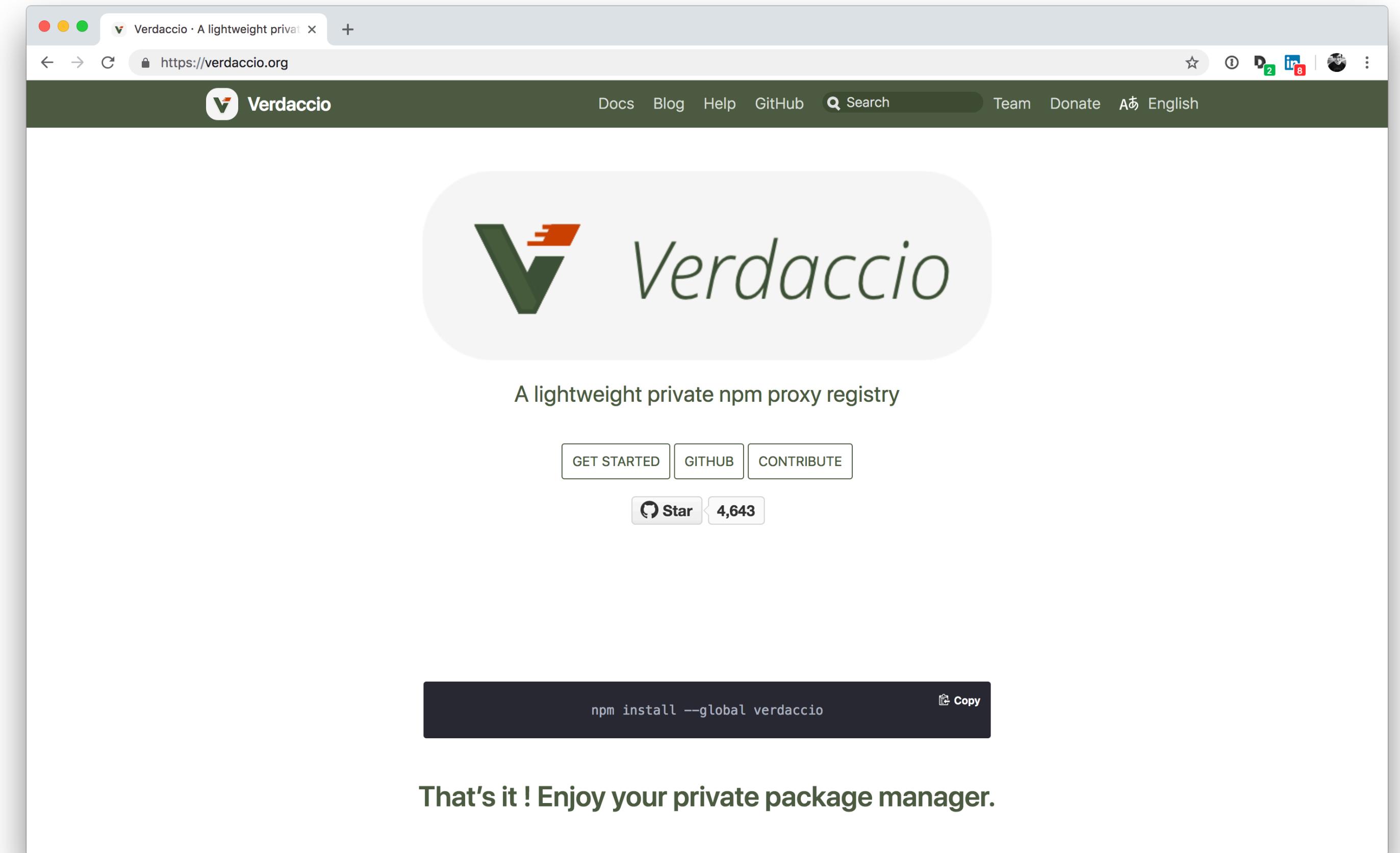
# Cache Locally & Publish Privately

# Verdaccio

Entirely open-source solution to private publishing. Fantastic, zero-cost\* solution.

\* If you want to support the continued development of

Verdaccio, they have an OpenCollective: [opencollective.com/verdaccio](https://opencollective.com/verdaccio)



# Monitor for Vulnerabilities

npm audit / Snyk / CVEs / Node.js Security WG

# Monitor for Vulnerabilities

## npm audit

Formerly *Node Security Platform* from Lift<sup>^</sup>

Security, npm audit is built directly into the npm  
CLI.

```
~/github/goof
→ goof git:(master) ✘ npm audit
    === npm audit security report ===
# Run npm install marked@0.5.1 to resolve 2 vulnerabilities


| High          | Sanitization bypass using HTML Entities                                                     |
|---------------|---------------------------------------------------------------------------------------------|
| Package       | marked                                                                                      |
| Dependency of | marked                                                                                      |
| Path          | marked                                                                                      |
| More info     | <a href="https://nodesecurity.io/advisories/101">https://nodesecurity.io/advisories/101</a> |


| High          | Regular Expression Denial of Service                                                        |
|---------------|---------------------------------------------------------------------------------------------|
| Package       | marked                                                                                      |
| Dependency of | marked                                                                                      |
| Path          | marked                                                                                      |
| More info     | <a href="https://nodesecurity.io/advisories/531">https://nodesecurity.io/advisories/531</a> |

# Run npm install adm-zip@0.4.11 to resolve 1 vulnerability


| High          | Arbitrary File Write via Archive Extraction                                                 |
|---------------|---------------------------------------------------------------------------------------------|
| Package       | adm-zip                                                                                     |
| Dependency of | adm-zip                                                                                     |
| Path          | adm-zip                                                                                     |
| More info     | <a href="https://nodesecurity.io/advisories/681">https://nodesecurity.io/advisories/681</a> |

# Run npm install errorhandler@1.5.0 to resolve 1 vulnerability


| High          | Regular Expression Denial of Service                                                        |
|---------------|---------------------------------------------------------------------------------------------|
| Package       | negotiator                                                                                  |
| Dependency of | errorhandler                                                                                |
| Path          | errorhandler > accepts > negotiator                                                         |
| More info     | <a href="https://nodesecurity.io/advisories/106">https://nodesecurity.io/advisories/106</a> |


```

# Monitor for Vulnerabilities

# Snyk

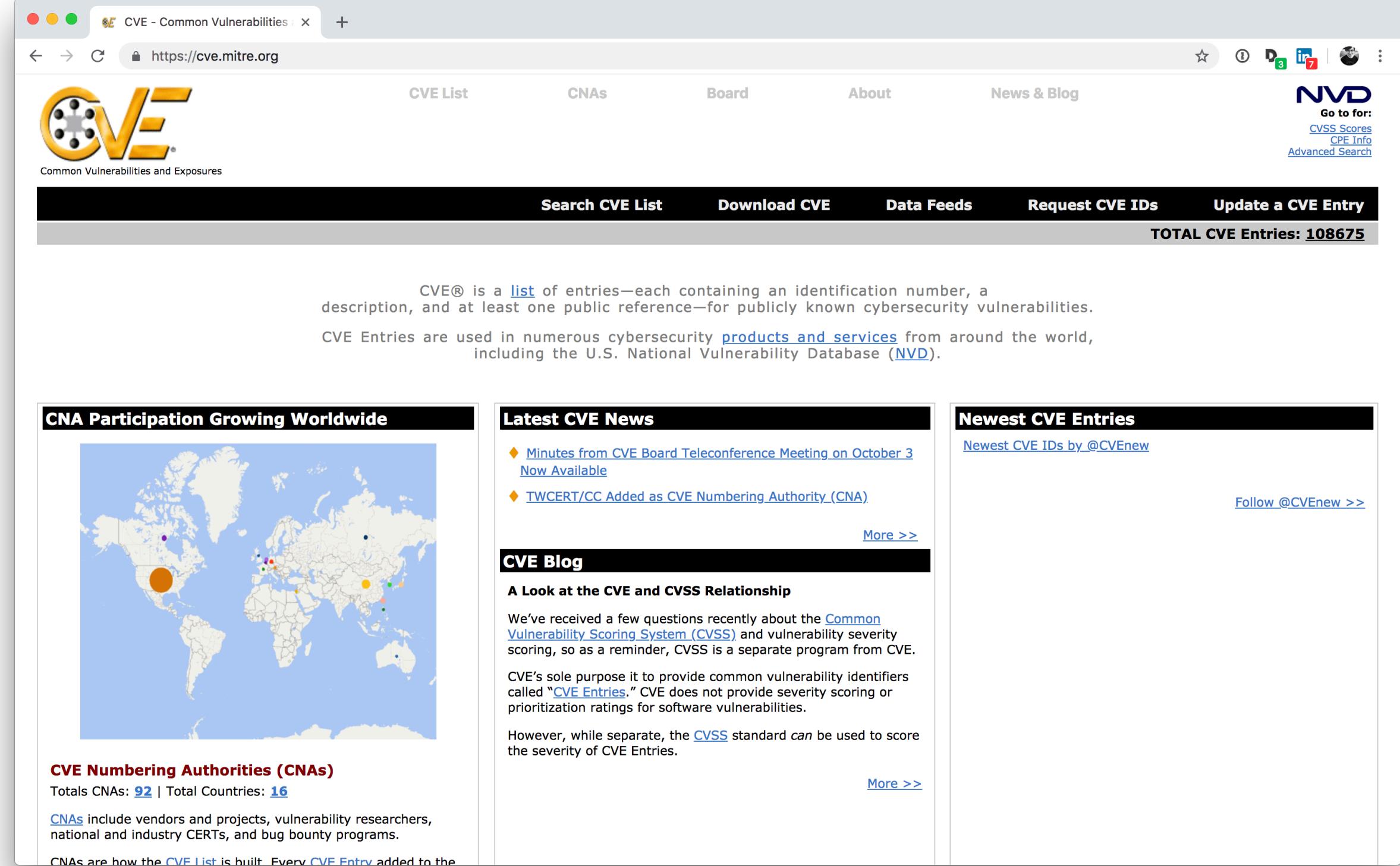
Largest database of all kinds of Node.js and JavaScript vulnerabilities in npm, all available in machine-consumable methods to paid users.

The screenshot shows the Snyk web interface for the project 'nodekitten'. The top navigation bar includes 'Dashboard', 'Reports', 'Projects' (which is selected), 'Integrations', and 'Settings'. The user 'Tierney Cyren' is logged in. The main content area displays the project name 'nodekitten' and a message indicating a 'Snapshot taken using v10.8.0, a day ago.' It shows 0 vulnerabilities via 0 paths, 63 dependencies, and the host is TLCs-MacBook-Pro.local. A sidebar on the left allows filtering by severity (High, Medium, Low) and status (Patched, Ignored). A message states 'No known vulnerabilities found' and notes that badges currently only work for public npm packages and open source GitHub repositories. The bottom of the page includes copyright information (© 2018 Snyk Ltd.) and links to API Status, Vulnerability DB, Blog, and Documentation.

# Monitor for Vulnerabilities

## CVEs

CVEs technically hold all known Node.js and npm vulnerabilities. Zero easy-win automation.



The screenshot shows the homepage of the CVE website at https://cve.mitre.org. The page features a navigation bar with links for 'CVE List', 'CNAs', 'Board', 'About', 'News & Blog', and social media icons. A prominent search bar is located below the navigation. The main content area includes a map titled 'CNA Participation Growing Worldwide' showing the locations of various CVE Numbering Authorities (CNAs) around the world. Below the map, there's a section about 'CVE Numbering Authorities (CNAs)' stating there are 92 total CNAs and 16 total countries. To the right, there are three columns: 'Latest CVE News' with two recent items, 'Newest CVE Entries' with a link to the latest IDs, and a 'CVE Blog' section with a link to more information. The top right corner of the page displays the NVD logo and links to CVSS Scores, CPE Info, and Advanced Search.

# Monitor for Vulnerabilities

## Node.js Security WG

The Node.js Security WG has the second largest vulnerability data set. The data includes ecosystem and Node.js core vulnerabilities.

nodejs / security-wg ✓

Code Issues Pull requests More Settings

Node.js Security Working Group

nodejs node Manage topics

316 commits 12 branches 0 releases 30 contributors MIT

Branch: master Create new file Find file Clone or download

Commit	Message	Time Ago
sam-github Request to re-join Security WG (#419) ...	Latest commit 2180728 19 hours ago	
.github	docs(processes) add triage-team-only offboarding checklist (#326)	4 months ago
meetings	doc: add minutes for meeting 4 Oct 2018 (#413)	11 days ago
processes	add Andreas to triage team (#406)	a month ago
tools	feat(reporter): add support for pulling CVE IDs for a report from the...	2 months ago
vuln	added nswg-eco-472 (#403)	27 days ago
.gitignore	Add CI to validate vulnerability format (#102)	7 months ago
.travis.yml	Enable Travis-ci on repo (#289)	5 months ago
CONTRIBUTING.md	Updated link to Code of conduct	a year ago
GOVERNANCE.md	Update GOVERNANCE.md (#367)	2 months ago
LICENSE.md	doc: Fix typo in license filename	a year ago
README.md	Request to re-join Security WG (#419)	19 hours ago
package-lock.json	feat(nswg-reporter): initial proposition for hackerone reporter (#234)	3 months ago
package.json	feat(nswg-reporter): initial proposition for hackerone reporter (#234)	3 months ago

All of these are development-time  
and CI/CD tools.

# Covering Your Apps in Production

What are the options?

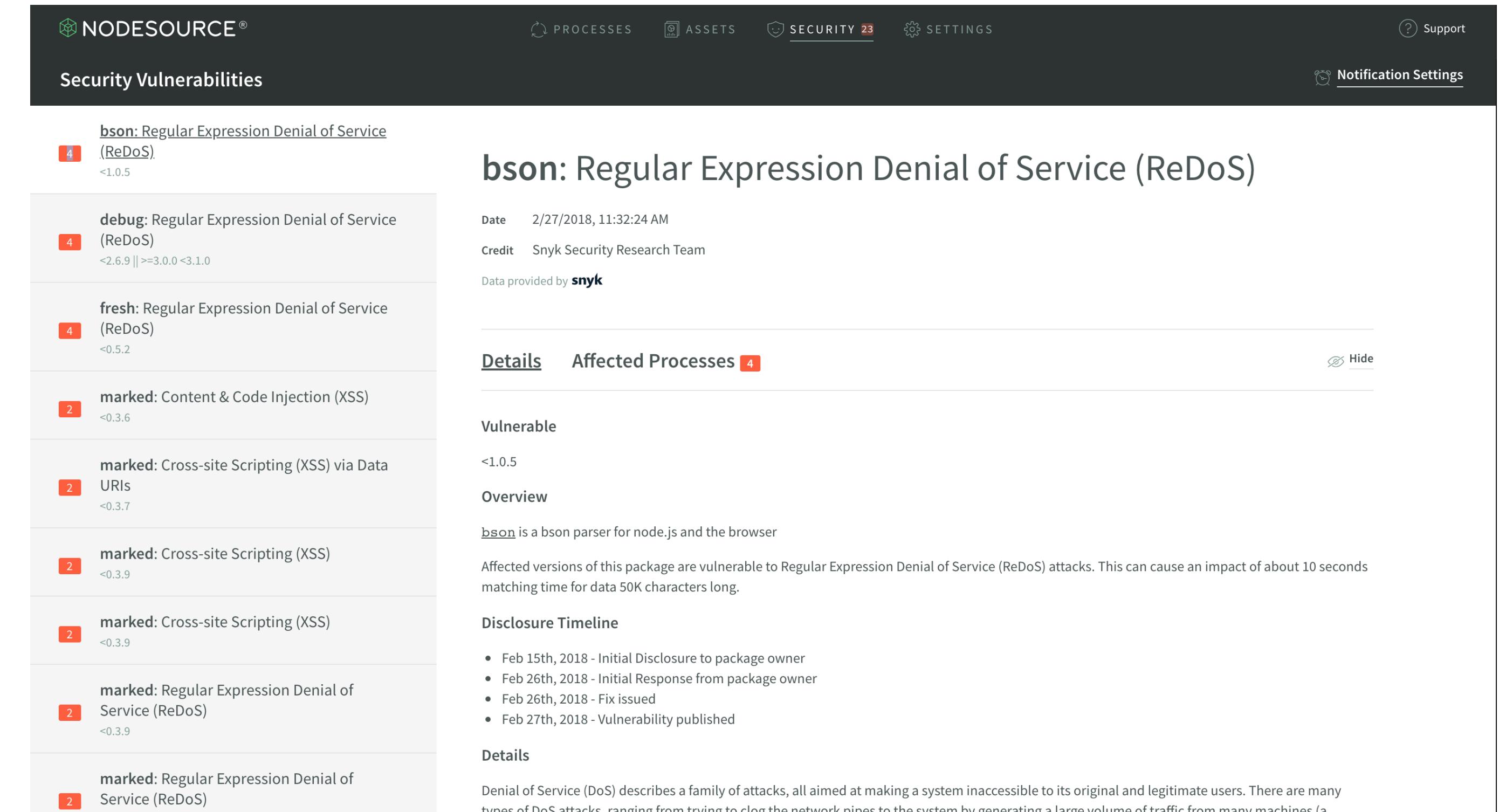
There aren't a lot!



# Covering Your Apps in Production

# N|Solid

Monitor your Node.js applications for top level and deeply nested security vulnerabilities, live in production.



The screenshot shows the NodeSource Security Vulnerabilities dashboard. At the top, there are navigation links: PROCESSES, ASSETS, SECURITY (with 23 notifications), SETTINGS, and a Support link. Below the navigation is a "Notification Settings" button. The main section is titled "Security Vulnerabilities" and lists vulnerabilities for the "bson" package:

Vulnerability Type	Package	Severity	Description
Regular Expression Denial of Service (ReDoS)	bson	4	Regular Expression Denial of Service (ReDoS) <1.0.5
Regular Expression Denial of Service (ReDoS)	debug	4	Regular Expression Denial of Service (ReDoS) <2.6.9    >=3.0.0 <3.1.0
Regular Expression Denial of Service (ReDoS)	fresh	4	Regular Expression Denial of Service (ReDoS) <0.5.2
Content & Code Injection (XSS)	marked	2	Content & Code Injection (XSS) <0.3.6
Cross-site Scripting (XSS) via Data URLs	marked	2	Cross-site Scripting (XSS) via Data URLs <0.3.7
Cross-site Scripting (XSS)	marked	2	Cross-site Scripting (XSS) <0.3.9
Cross-site Scripting (XSS)	marked	2	Cross-site Scripting (XSS) <0.3.9
Regular Expression Denial of Service (ReDoS)	marked	2	Regular Expression Denial of Service (ReDoS) <0.3.9
Regular Expression Denial of Service (ReDoS)	marked	2	Regular Expression Denial of Service (ReDoS)

On the right side, a detailed view of the first vulnerability is shown:

**bson: Regular Expression Denial of Service (ReDoS)**

Date: 2/27/2018, 11:32:24 AM  
Credit: Snyk Security Research Team  
Data provided by snyk

**Details** **Affected Processes** 4

**Vulnerable**  
<1.0.5

**Overview**  
**bson** is a bson parser for node.js and the browser  
Affected versions of this package are vulnerable to Regular Expression Denial of Service (ReDoS) attacks. This can cause an impact of about 10 seconds matching time for data 50K characters long.

**Disclosure Timeline**

- Feb 15th, 2018 - Initial Disclosure to package owner
- Feb 26th, 2018 - Initial Response from package owner
- Feb 26th, 2018 - Fix issued
- Feb 27th, 2018 - Vulnerability published

**Details**  
Denial of Service (DoS) describes a family of attacks, all aimed at making a system inaccessible to its original and legitimate users. There are many types of DoS attacks ranging from trying to close the network pipes to the system by generating a large volume of traffic from many machines /a

What can you do to

# Cover Your Apps While Still Using npm?

Development Time:

**Set up a Registry Mirror as a Fallback**

**Cache Locally & Publish Privately**

**Monitor for Vulnerabilities**

Production:

**N|Solid**

# Thank you.

**Tierney Cyren**

[tierney@nodesource.com](mailto:tierney@nodesource.com)

@bitandbang



NODESOURCE®