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

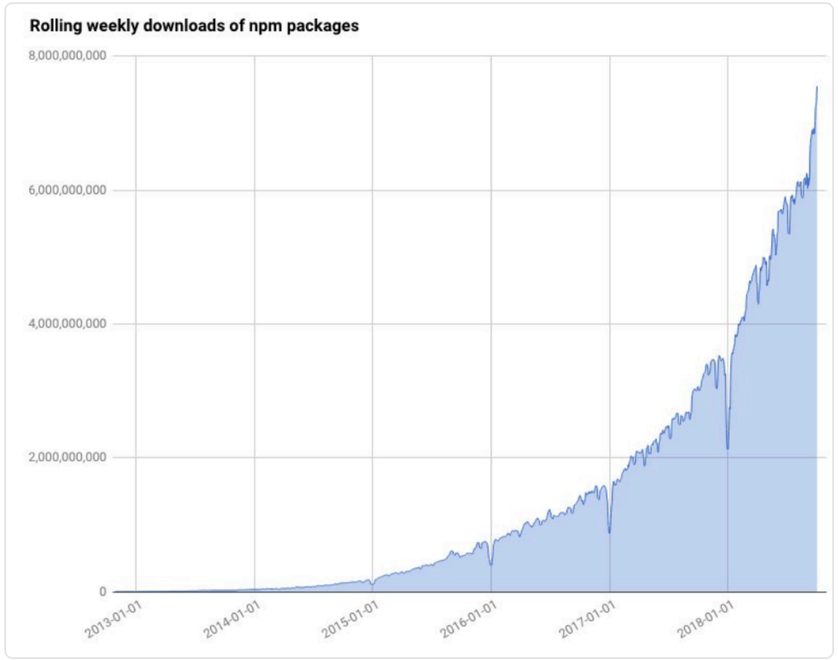
6,500,000,000 downloads last week

26,500,000,000 downloads last month

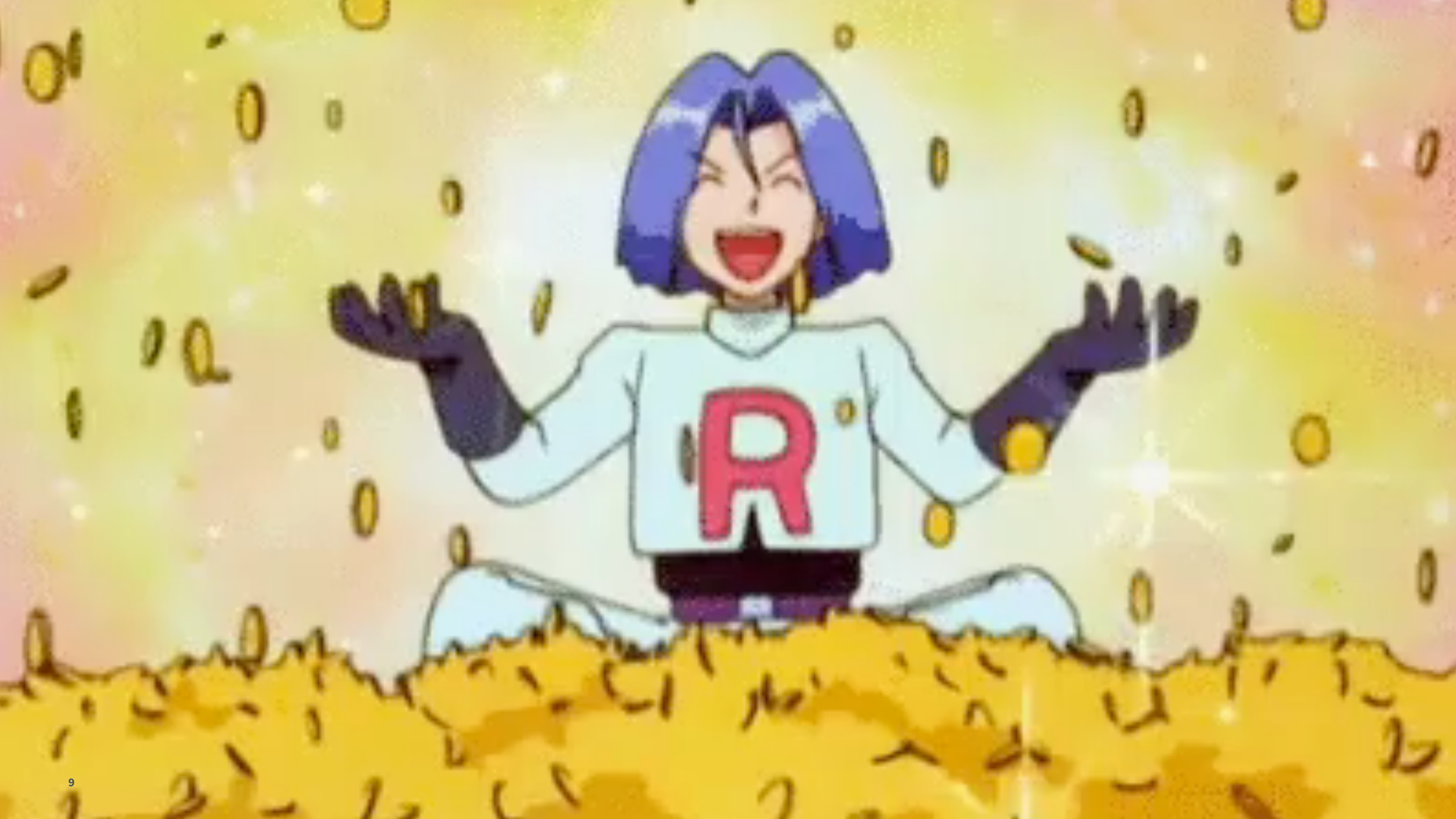
Laurie Voss
@seldo

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


R

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

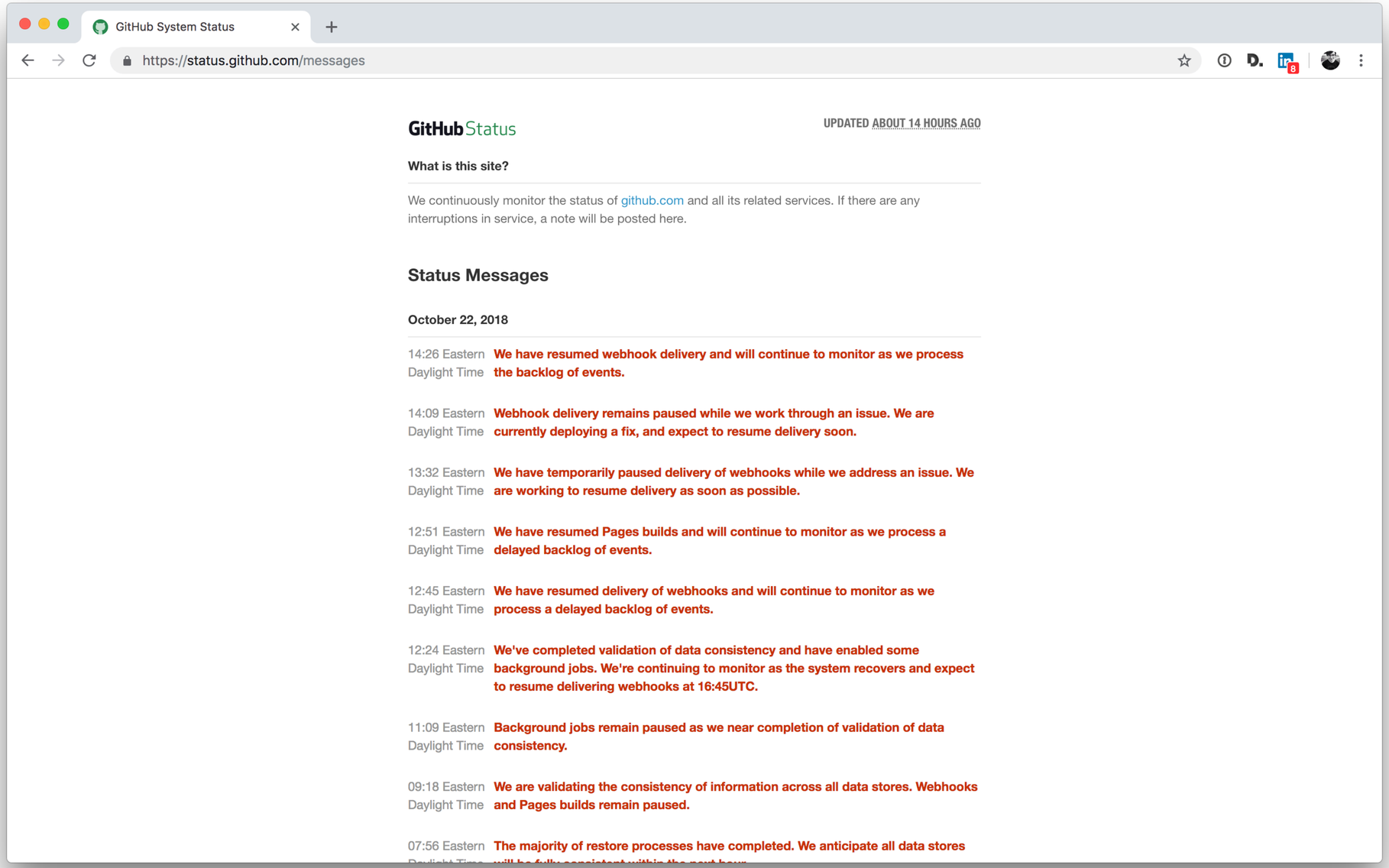
credit: webcomicname.com / @dorrismccomics / npmjs.com / @npmjs

We have a large and diverse ecosystem

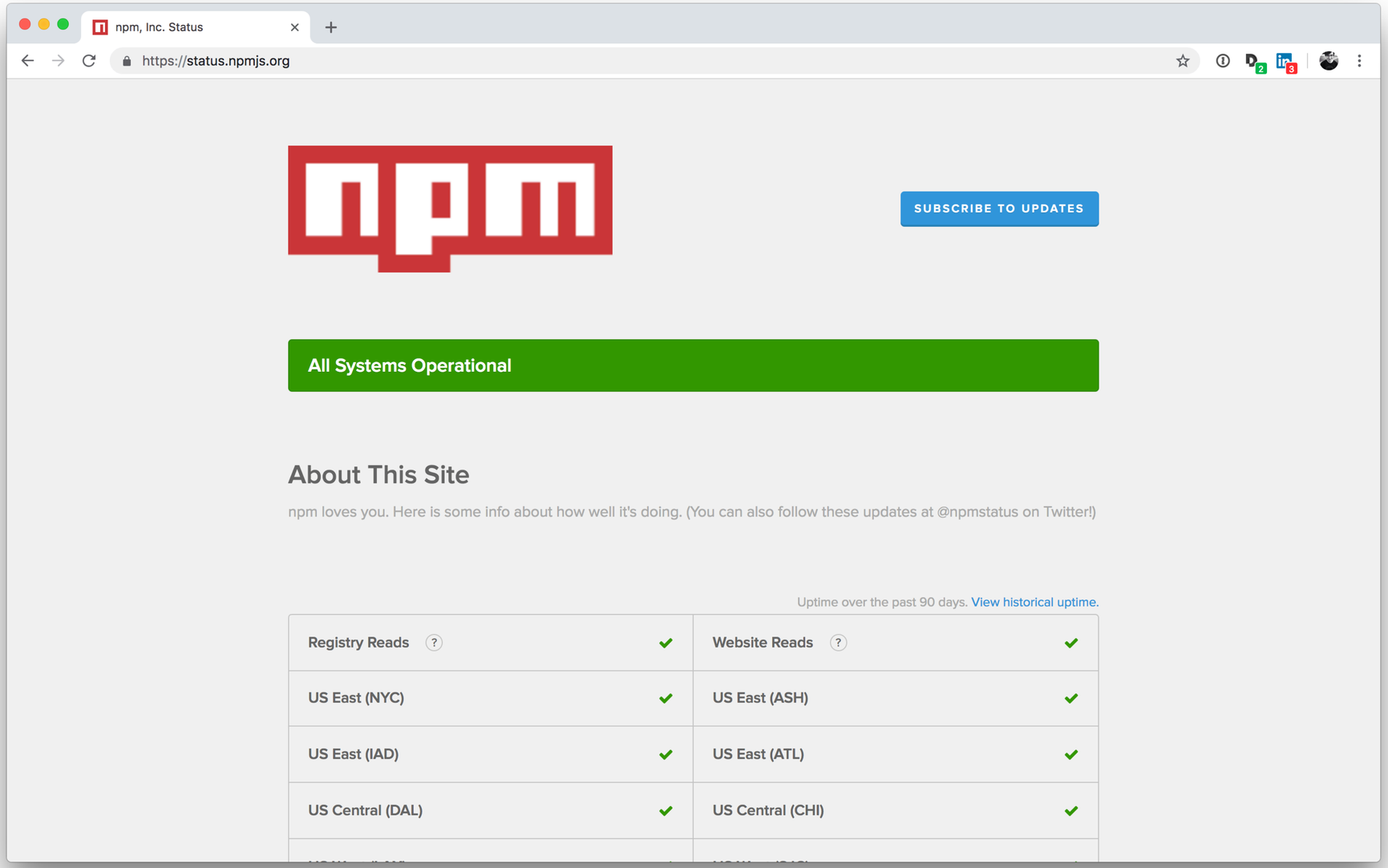
- There's *probably* multiple modules to do what you want
  - How do you choose?
- How can you know you trust all the modules you're using?
  - Do you even **know** all the modules you're using?
- What tools can you use to ensure you're shipping secure code?
- What do you do when there's an outage?

Software Repositories are Key Internet Infrastructure

How many of you trust GitHub?


GitHub System Status
https://status.github.com/messages
GitHub Status
UPDATED ABOUT 14 HOURS AGO
What is this site?
We continuously monitor the status of github.com and all its related services. If there are any interruptions in service, a note will be posted here.
Status Messages
October 22, 2018
14:26 Eastern Daylight Time We have resumed webhook delivery and will continue to monitor as we process the backlog of events.
14:09 Eastern Daylight Time Webhook delivery remains paused while we work through an issue. We are currently deploying a fix, and expect to resume delivery soon.
13:32 Eastern Daylight Time We have temporarily paused delivery of webhooks while we address an issue. We are working to resume delivery as soon as possible.
12:51 Eastern Daylight Time We have resumed Pages builds and will continue to monitor as we process a delayed backlog of events.
12:45 Eastern Daylight Time We have resumed delivery of webhooks and will continue to monitor as we process a delayed backlog of events.
12:24 Eastern Daylight Time We've completed validation of data consistency and have enabled some background jobs. We're continuing to monitor as the system recovers and expect to resume delivering webhooks at 16:45UTC.
11:09 Eastern Daylight Time Background jobs remain paused as we near completion of validation of data consistency.
09:18 Eastern Daylight Time We are validating the consistency of information across all data stores. Webhooks and Pages builds remain paused.
07:56 Eastern The majority of restore processes have completed. We anticipate all data stores

How many of you trust npm?


npm, Inc. Status
https://status.npmjs.org
SUBSCRIBE TO UPDATES
All Systems Operational
About This Site
npm loves you. Here is some info about how well it's doing. (You can also follow these updates at @npmstatus on Twitter!)
Uptime over the past 90 days. View historical uptime.
Registry Reads
Website Reads
US East (NYC)
US East (ASH)
US East (IAD)
US East (ATL)
US Central (DAL)
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 to to cover your apps?

Set up a Registry Mirror as a Fallback

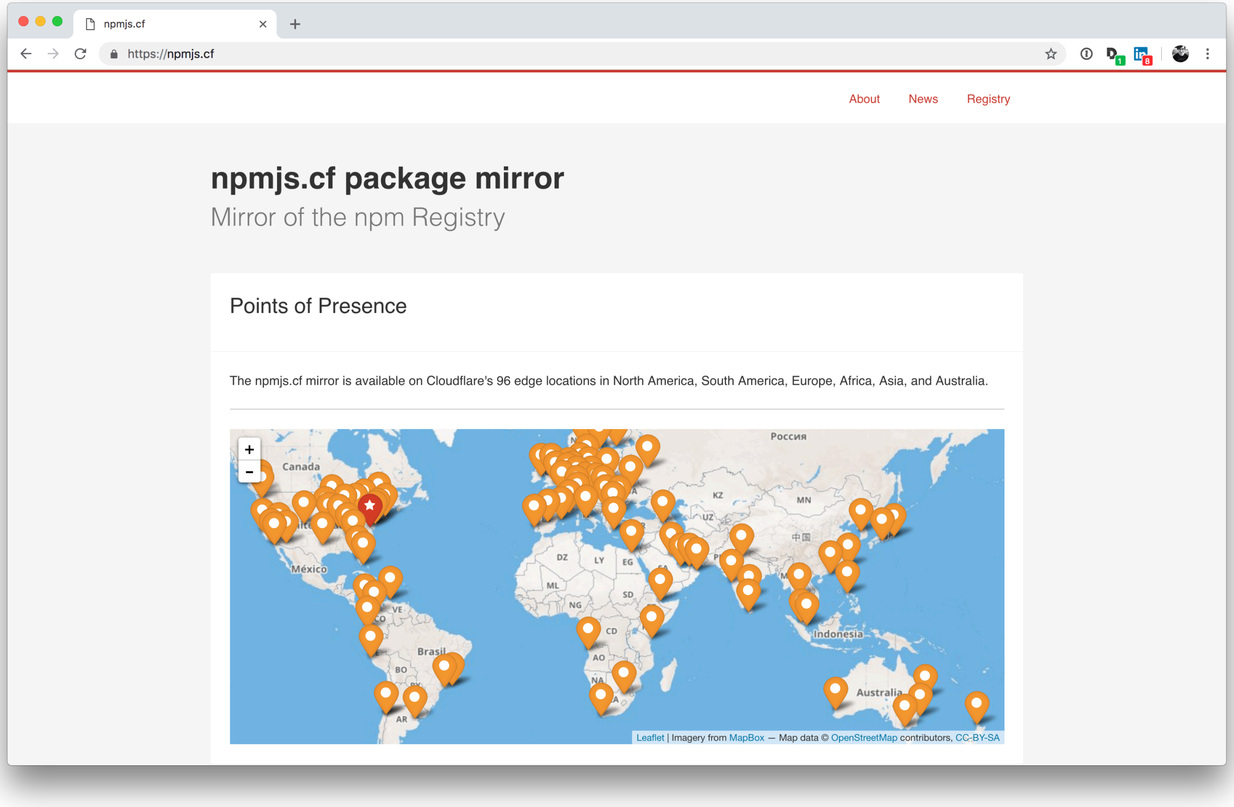
npmjs.cf / cnpmjs.org / roll your own

Set up a Registry Mirror as a Fallback

npmjs.cf

npm registry mirror on CloudFlare,

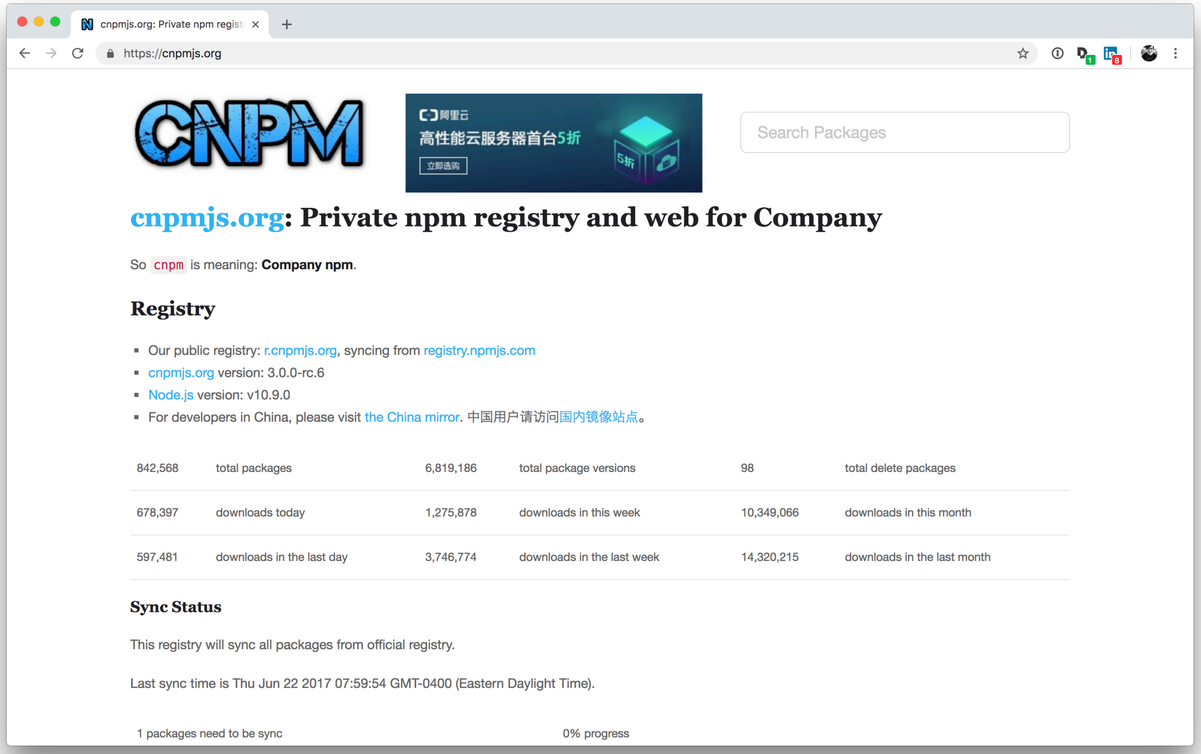
maintained by a CloudFlare employee.



Set up a Registry Mirror as a Fallback

cnpmjs.org

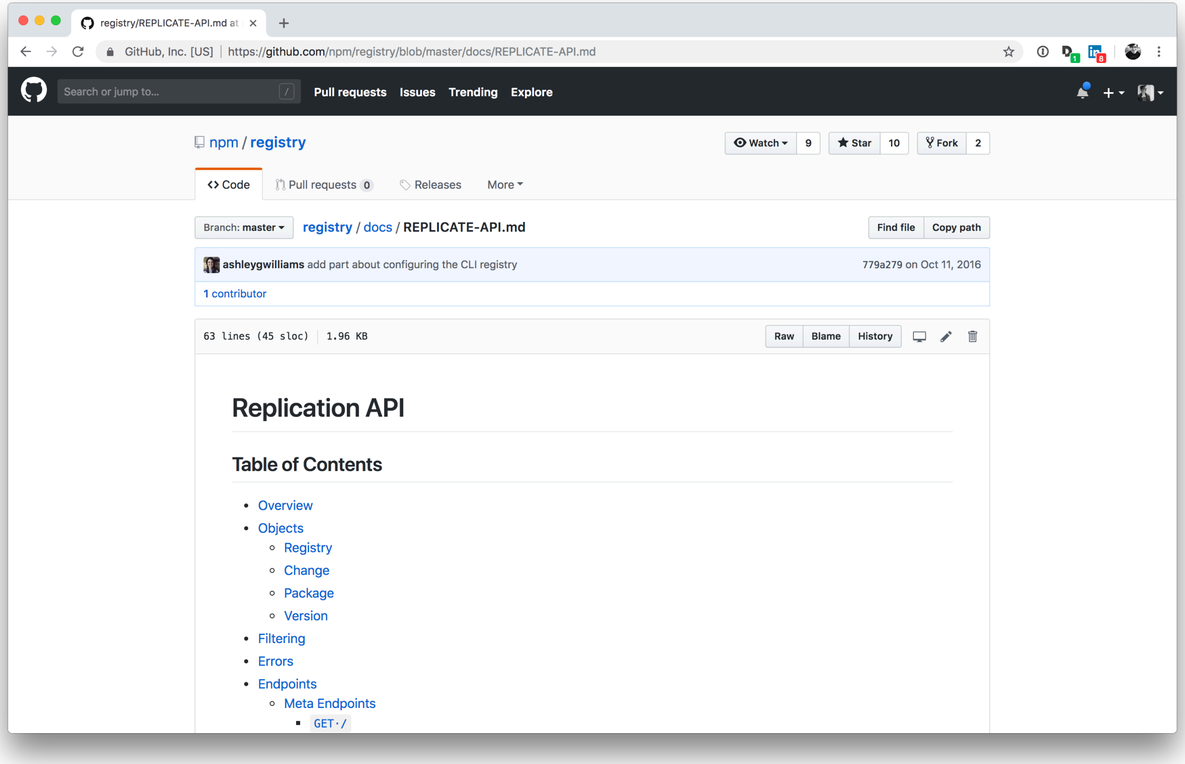
Chinese mirror of the npm registry, originally used by JavaScript developers in China as a solution for ensuring there aren't issues between the Great Firewall and npmjs.com.



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

Cache Locally &
Publish Privately

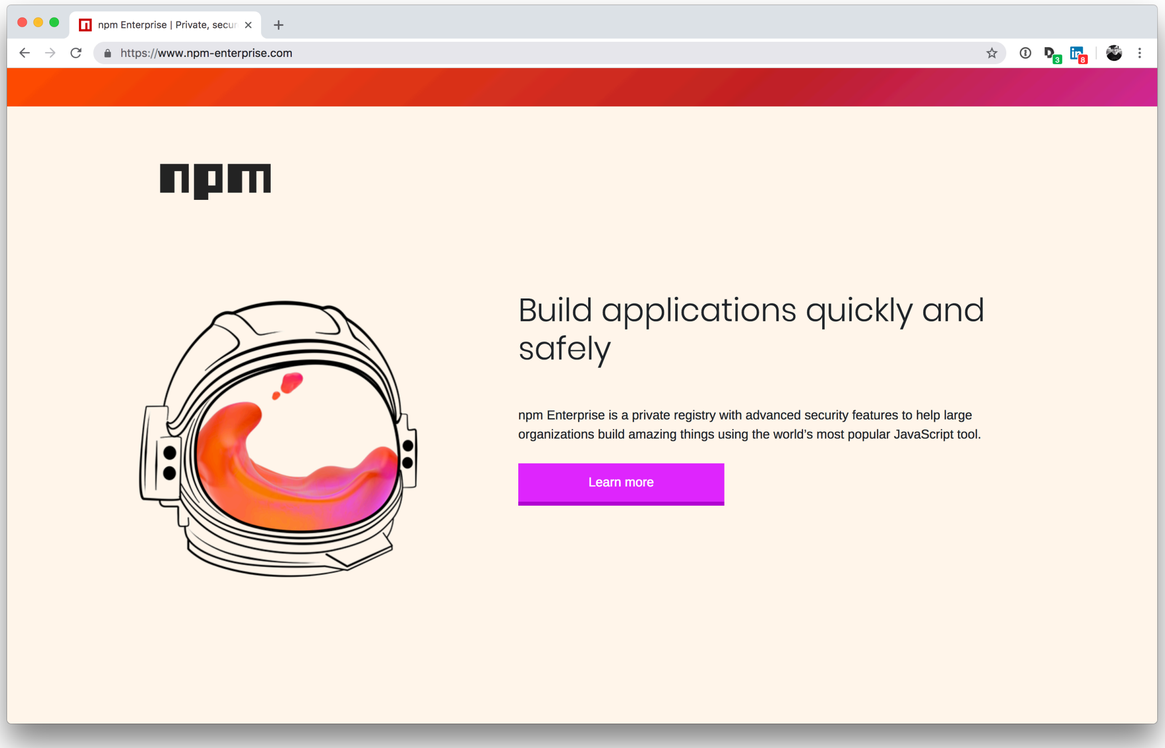
Enterprises: npm Enterprise / jFrog Artifactory

Developers/DIY: Verdaccio / Git / local-npm

Cache Locally & Publish Privately

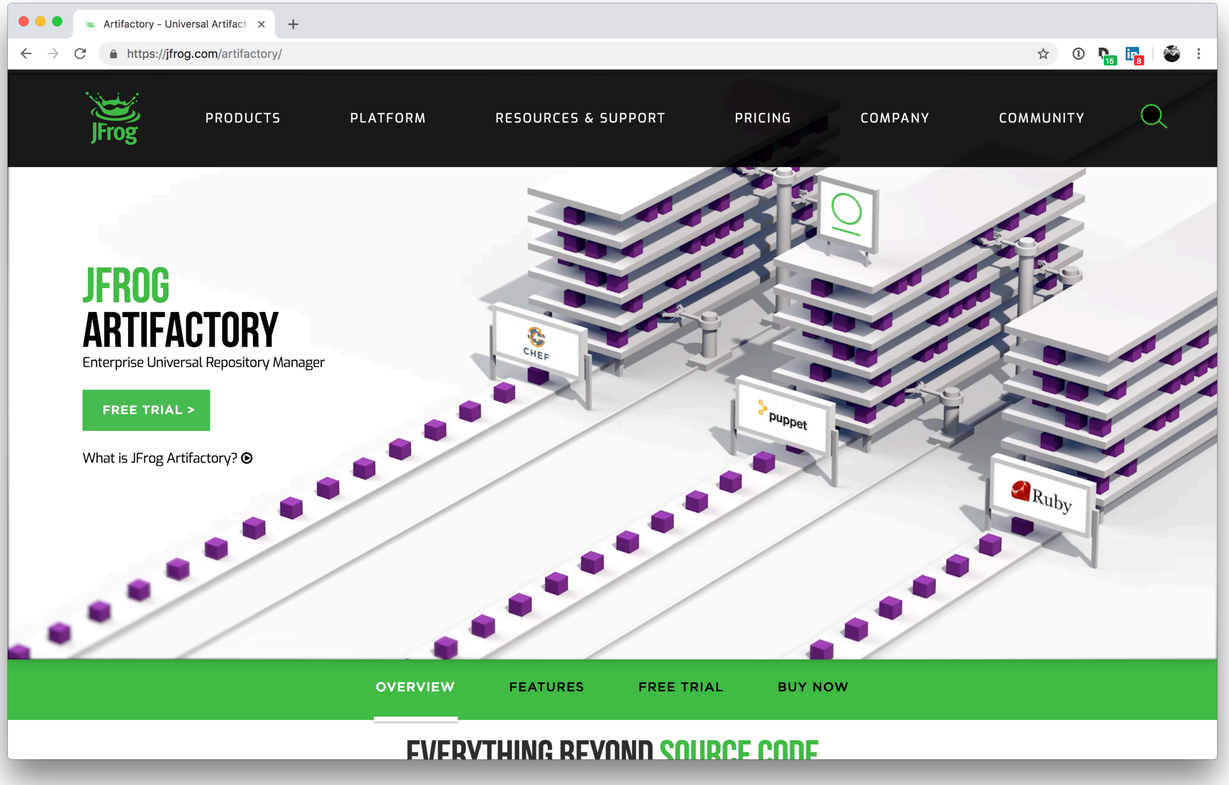
npm Enterprise

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



jFrog Artifactory

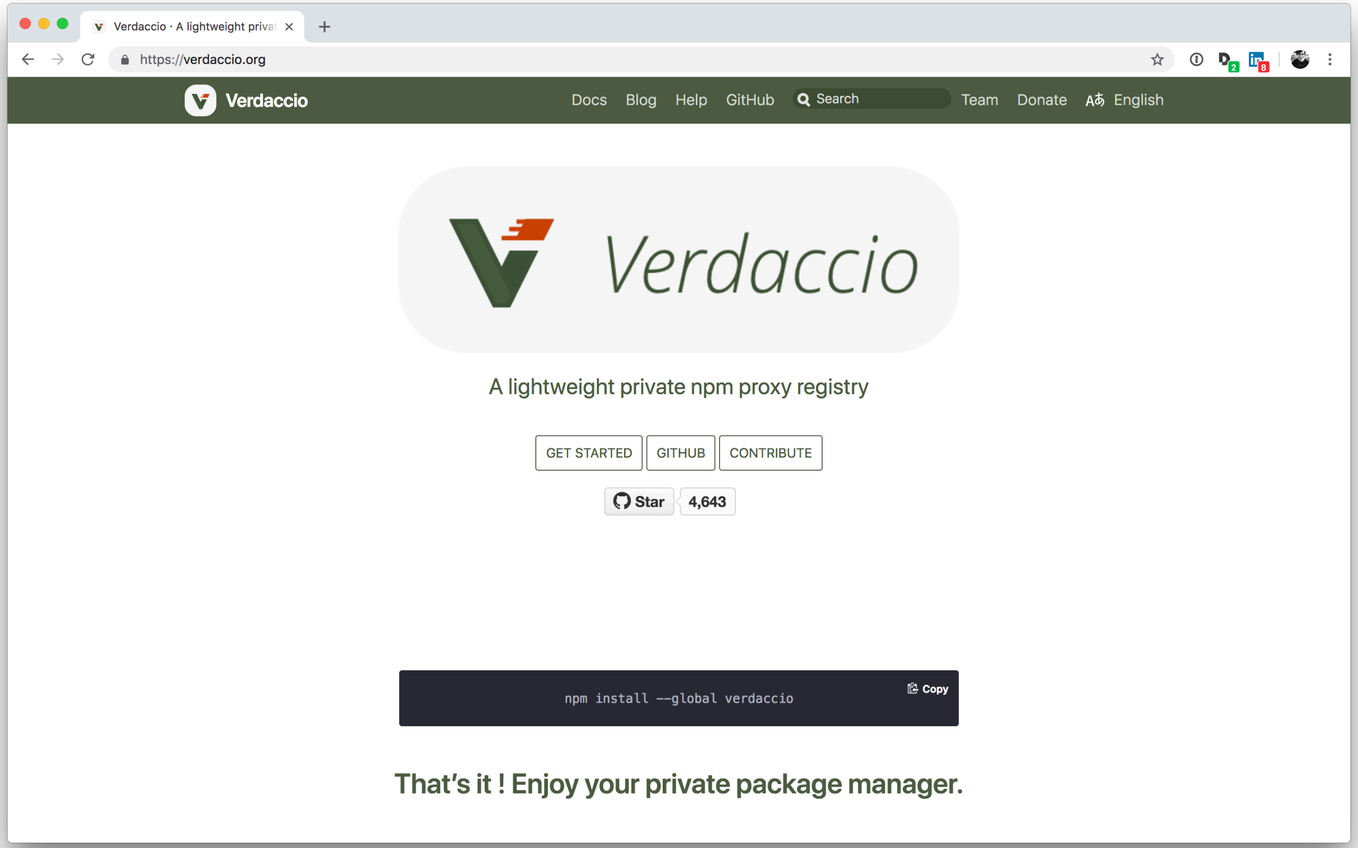
jFrog's solution to a private registry. If you already have Artifactory, this is a quick and easy win.



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



Monitor for Vulnerabilities

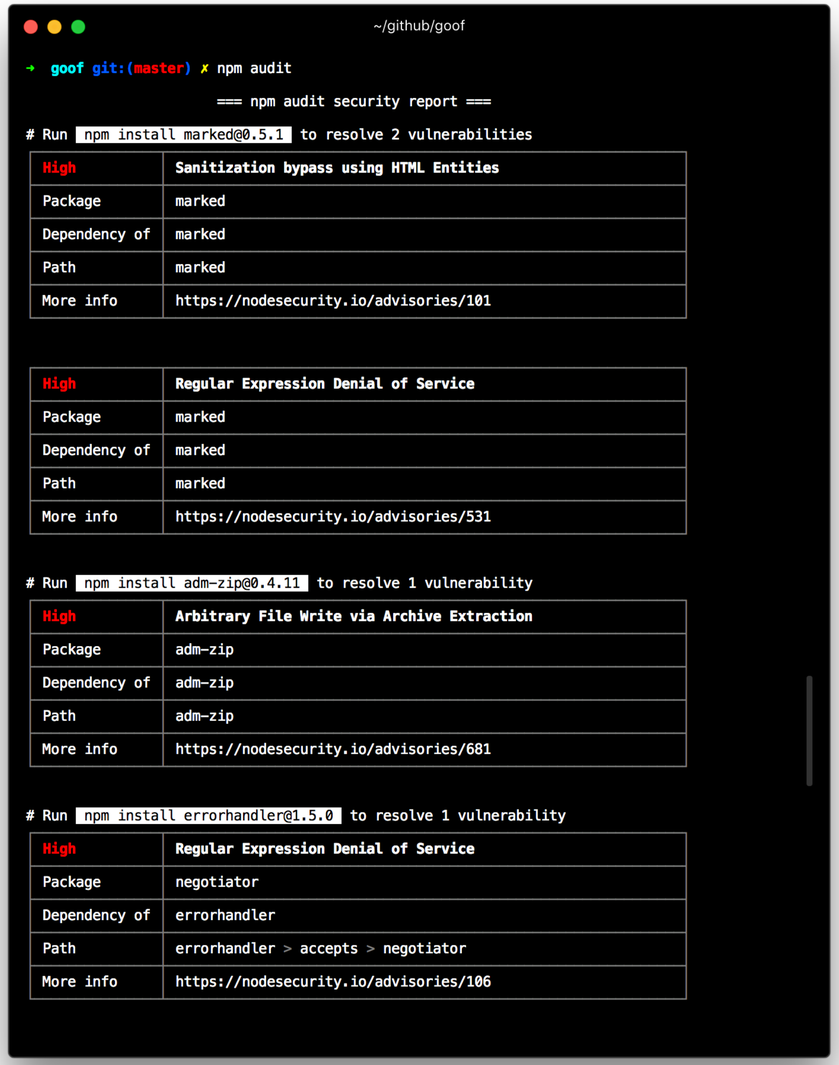
npm audit / Snyk / CVEs / Node.js Security WG

Monitor for Vulnerabilities

npm audit

Formerly *Node Security Platform* from Lift^

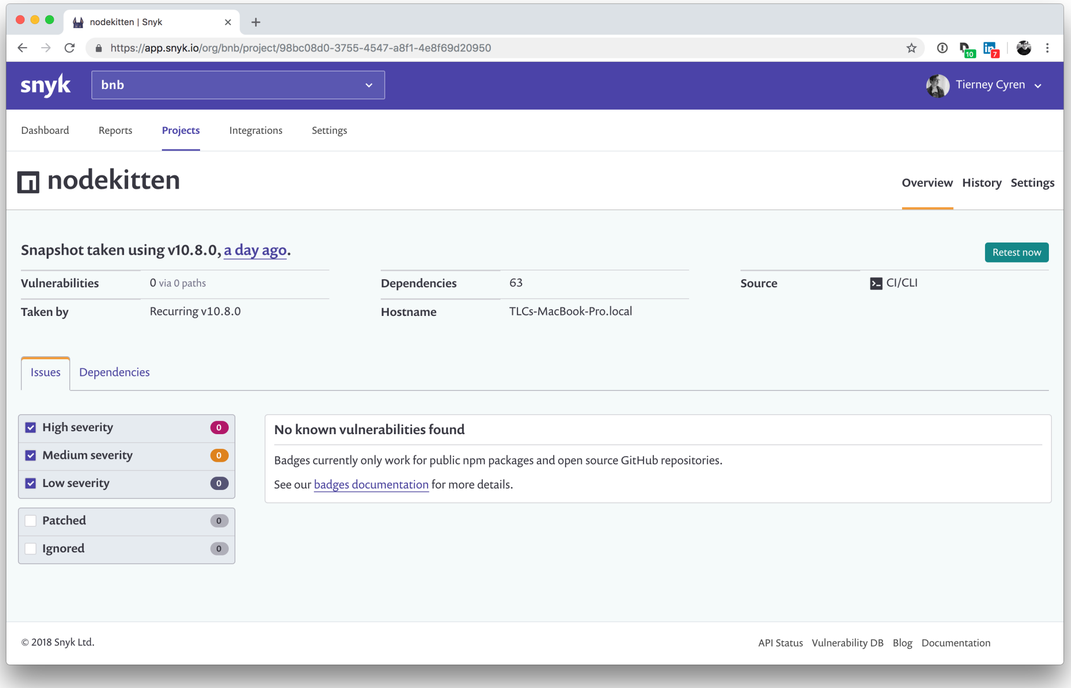
Security, npm audit is built directly into the npm CLI.



Monitor for Vulnerabilities

Snyk

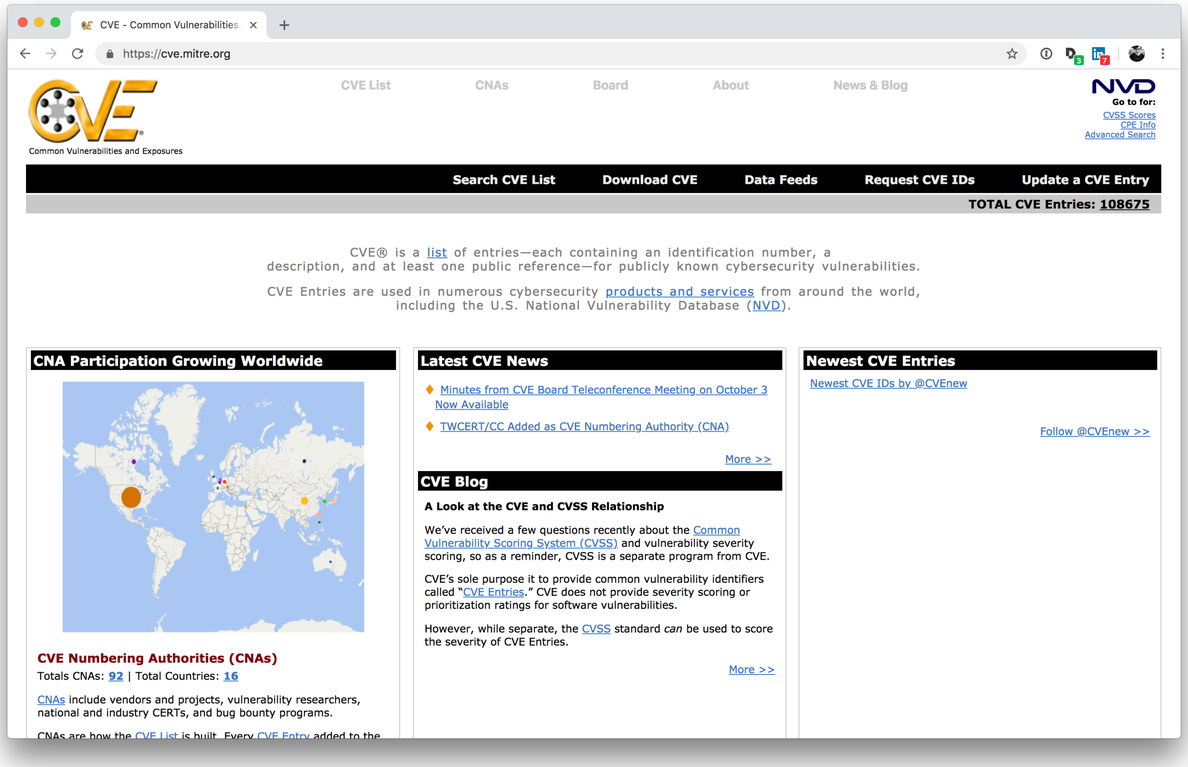
Largest database of all kinds of Node.js and JavaScript vulnerabilities in npm, all available in machine-consumable methods to paid users.



Monitor for Vulnerabilities

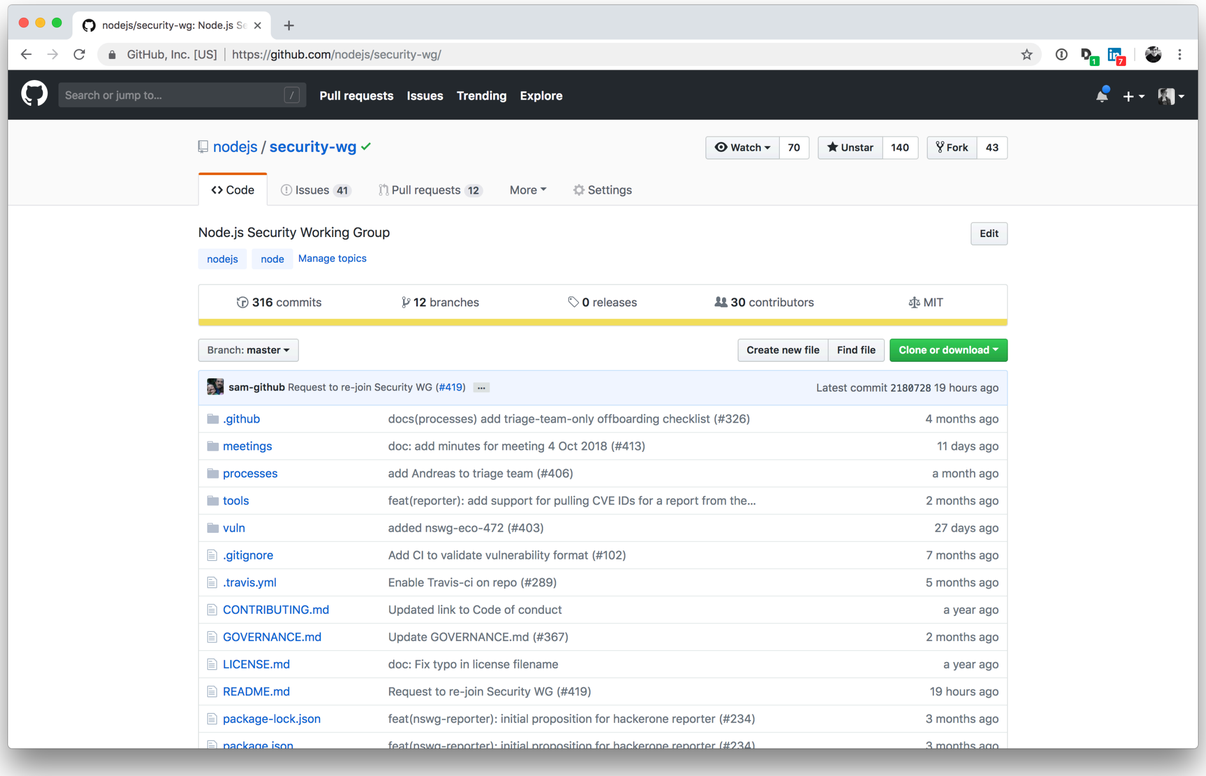
CVEs

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



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.



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

Covering Your Apps in Production

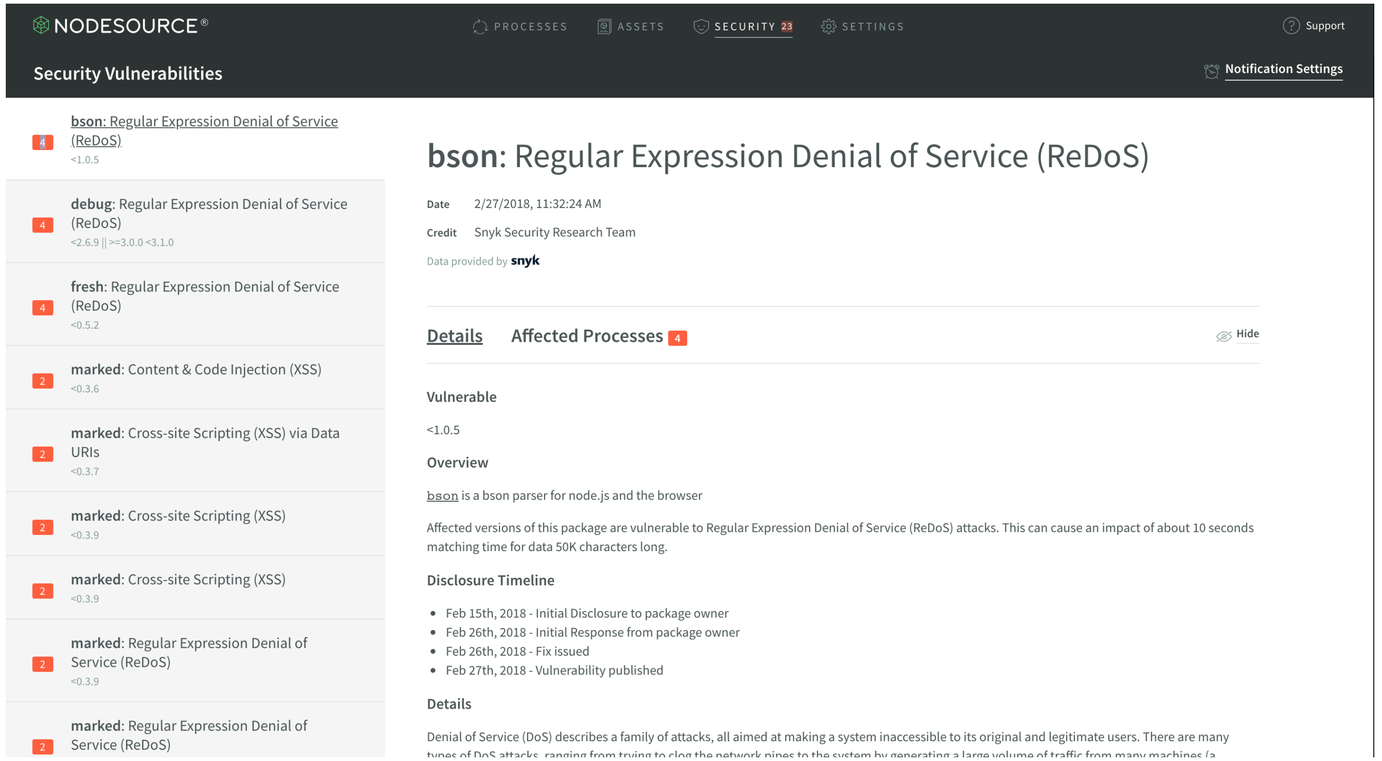
What are the options?

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.



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

@bitandbang

NODESOURCE®