Modernizing Supply Chain **Security**

tinyurl.com/**modern-2025**

Darcy Clarke

Based in **Toronto, Ontario, Canada** 🇨🇦

Founder & CEO

Member
OpenJS Foundation

Collaborator
Node.js WGs

npm · Themify · Deloitte. · TELUS

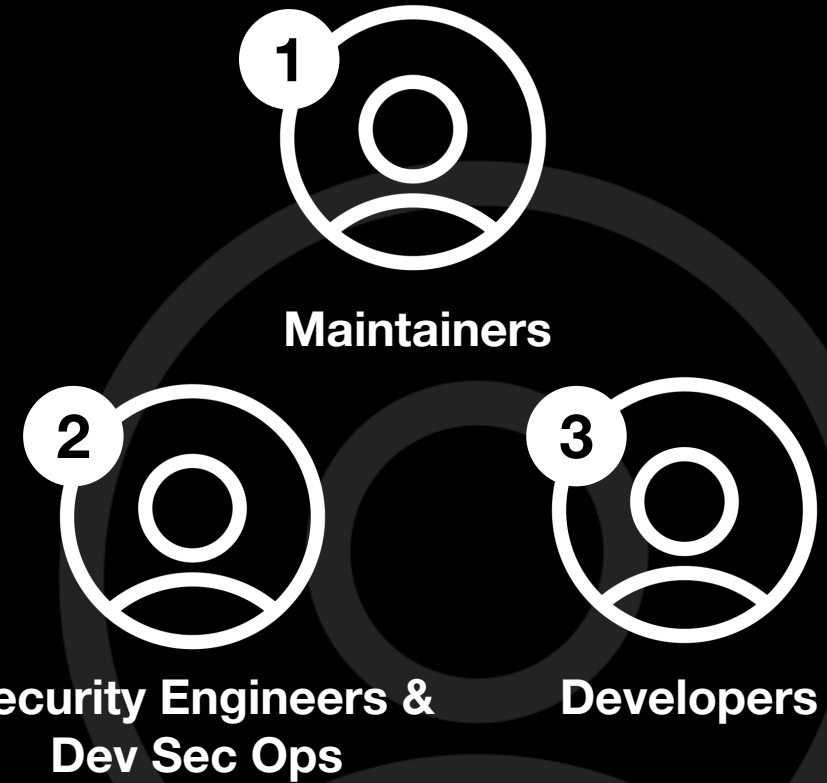
Google · Microsoft · CBS · Ducati · Porsche

Nike · Disney · Samsung · Panasonic · Burton

Red Bull · IAMS · Nestlé · The Lincoln Motor Company · facebook

Who

Are you?


1
Maintainers
2
Security Engineers &
Dev Sec Ops
3
Developers

Current State

Ecosystem

JS

Runtimes	
Runtime Managers	 n fnm nvs nodeenv nave asdf
Bundlers	
CI/CD Automation & Security	
Private Registries	
Monorepos & Build Pipelines	
Package Managers	
Public Registries	
Open Source Registries	

JS

Runtimes

Runtime Managers

n fnm nvs nodeenv nave asdf

Bundlers

CI/CD Automation & Security

Private Registries

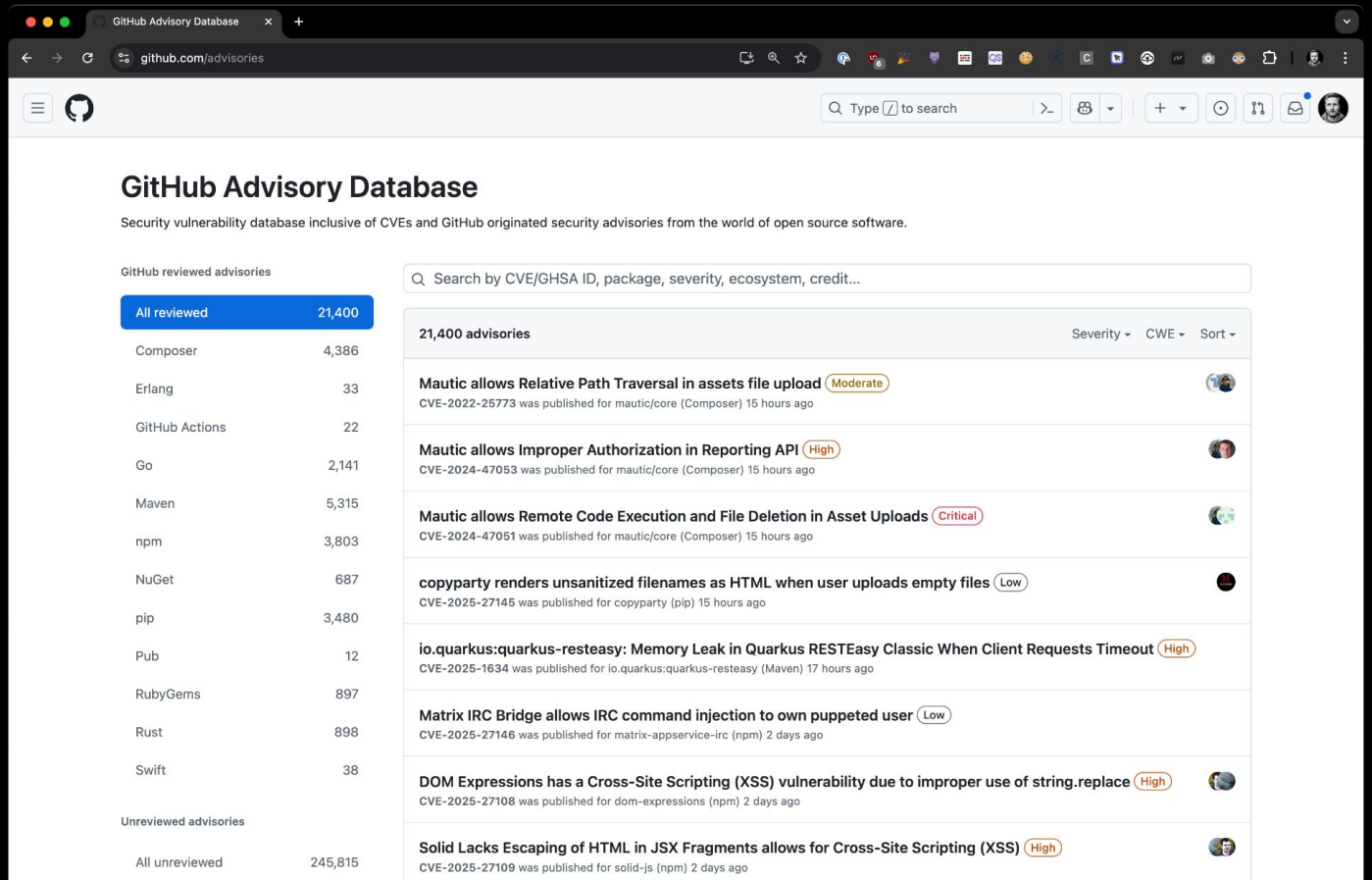
Monorepos & Build Pipelines

Package Managers

Public Registries

Open Source Registries

CVEs - Common Vulnerabilities & Exposures

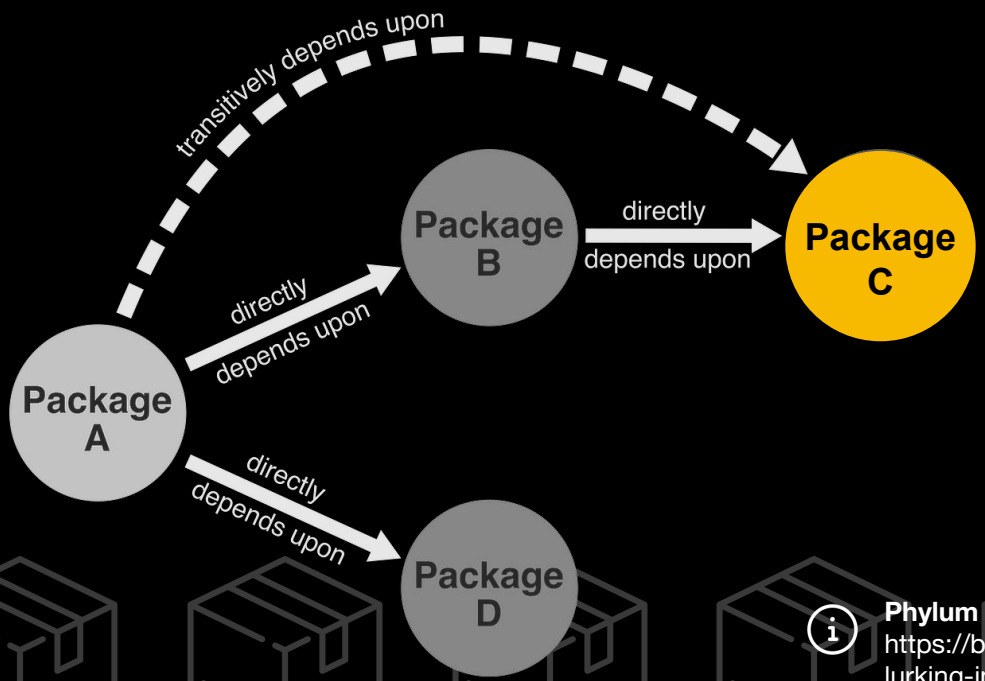


```
~/desktop/test/test-pkg (0.888s)
npm i

removed 2 packages, and audited 122 packages in 783ms

14 packages are looking for funding
  run `npm fund` for details

9 vulnerabilities (2 low, 3 moderate, 3 high, 1 critical)

To address all issues possible (including breaking changes), run:
  npm audit fix --force

Some issues need review, and may require choosing
a different dependency.

Run `npm audit` for details.
```

It’s estimated **75%**
of vulnerabilities reside in
transitive dependencies

Snyk’s State of Open Source Security 2020:
https://snyk.io/series/open-source-security/report-2020/

Transitive Dependencies



Phylum Blog Post
https://blog.phylum.io/hidden-dependencies-lurking-in-the-software-dependency-network

742%

year-over-year increase in attacks targeting the open source supply chain

Sonatype's State of Software Supply Chain Security 2022:
https://www.sonatype.com/state-of-the-software-supply-chain/

What are they

Exploiting?

- **Vulnerabilities**
- **Typosquatting**
- **Dependency/Manifest Confusion**
- **Registry Compromise**
- **Account Takeovers**
- **Malware**

How can we mitigate

Vulnerabilities

- **CVEs**
- **Active Scanning Tools**
- **Write better code**

Example: `create-react-app`

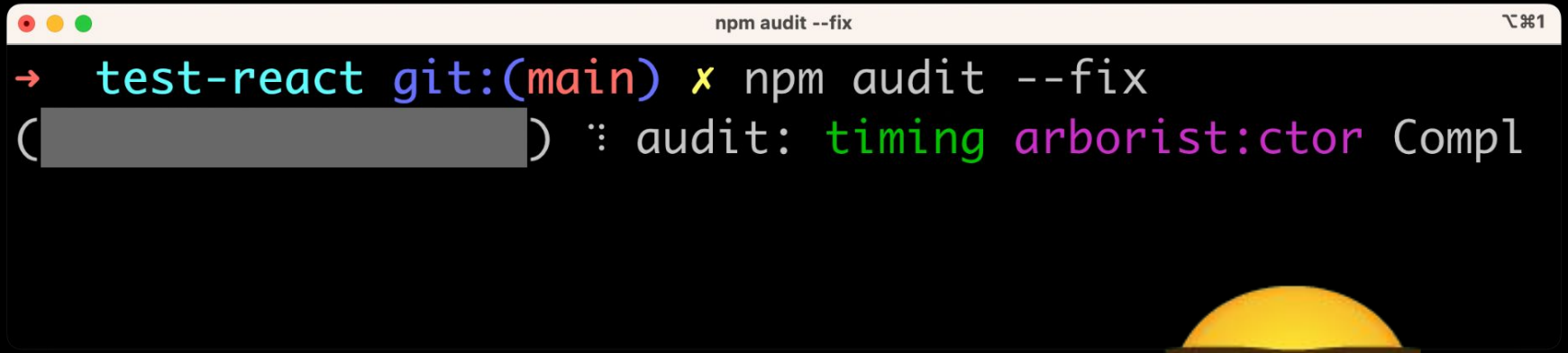
```
→  test-react git:(main) ✗ npm audit
# npm audit report

nth-check  <2.0.1
Severity: high
Inefficient Regular Expression Complexity in nth-check - https://github.com/advisories/GHSA-rp65-9cf3-cjxr
fix available via `npm audit fix --force`
Will install react-scripts@2.1.3, which is a breaking change
node_modules/svgo/node_modules/nth-check
  css-select  <=3.1.0
  Depends on vulnerable versions of nth-check
  node_modules/svgo/node_modules/css-select
    svgo  1.0.0 - 1.3.2
    Depends on vulnerable versions of css-select
    node_modules/svgo
      @svgr/plugin-svgo  <=5.5.0
      Depends on vulnerable versions of svgo
      node_modules/@svgr/plugin-svgo
        @svgr/webpack  4.0.0 - 5.5.0
        Depends on vulnerable versions of @svgr/plugin-svgo
        node_modules/@svgr/webpack
          react-scripts  >=2.1.4
          Depends on vulnerable versions of @svgr/webpack
          node_modules/react-scripts

6 high severity vulnerabilities

To address all issues (including breaking changes), run:
  npm audit fix --force
```


I DON'T KNOW HOW TO USE NPM INSTALL WITHOUT GETTING 104 VULNERABILITIES
AND AT THIS POINT I'M TOO AFRAID TO ASK

Example: `create-react-app`

```
→  test-react git:(main) ✗ npm audit
# npm audit report

nth-check  <2.0.1
Severity: high
Inefficient Regular Expression Complexity in nth-check - https://github.com/advisories/GHSA-rp65-9cf3-cjxr
fix available via `npm audit fix --force`
Will install react-scripts@2.1.3, which is a breaking change
node_modules/svgo/node_modules/nth-check
  css-select  <=3.1.0
  Depends on vulnerable versions of nth-check
  node_modules/svgo/node_modules/css-select
    svgo  1.0.0 - 1.3.2
    Depends on vulnerable versions of css-select
    node_modules/svgo
      @svgr/plugin-svgo  <=5.5.0
      Depends on vulnerable versions of svgo
      node_modules/@svgr/plugin-svgo
        @svgr/webpack  4.0.0 - 5.5.0
        Depends on vulnerable versions of @svgr/plugin-svgo
        node_modules/@svgr/webpack
          react-scripts  >=2.1.4
          Depends on vulnerable versions of @svgr/webpack
          node_modules/react-scripts

6 high severity vulnerabilities

To address all issues (including breaking changes), run:
  npm audit fix --force
```

Example: `create-react-app`



```
Severity: high
Terser insecure use of regular expressions leads to ReDoS - https://github.com/advisories/GHSA-4wf5-vphf-c2xc
fix available via `npm audit fix --force`
Will install react-scripts@5.0.1, which is a breaking change
node_modules/terser

yargs-parser  6.0.0 - 13.1.1
Severity: moderate
yargs-parser Vulnerable to Prototype Pollution - https://github.com/advisories/GHSA-p9pc-299p-vxgp
fix available via `npm audit fix --force`
Will install react-scripts@5.0.1, which is a breaking change
node_modules/webpack-dev-server/node_modules/yargs-parser
node_modules/yargs-parser
  yargs  8.0.0-candidate.0 - 12.0.5
  Depends on vulnerable versions of yargs-parser
  node_modules/webpack-dev-server/node_modules/yargs
  node_modules/yargs

84 vulnerabilities (14 low, 19 moderate, 43 high, 8 critical)

To address issues that do not require attention, run:
  npm audit fix

To address all issues (including breaking changes), run:
  npm audit fix --force
```

Example: `create-react-app`


IT'S NOT WORKING

How can we mitigate

Typosquatting

- **Heuristics**
  (name, downloads, versions, published date, author etc.)
- **Policies & Enforcement**

How can we mitigate

Dependency Confusion

- **Use a publicly owned scope for internal/private proxied packages**
- **Set registry configuration in a `.npmrc` file at the root-level of your projects**
- **Respond quickly to build failures**
- **Introduce per-package registry protocol to package specifier**

Avoiding npm substitution attacks
https://github.blog/2021-02-12-avoiding-npm-substitution-attacks/

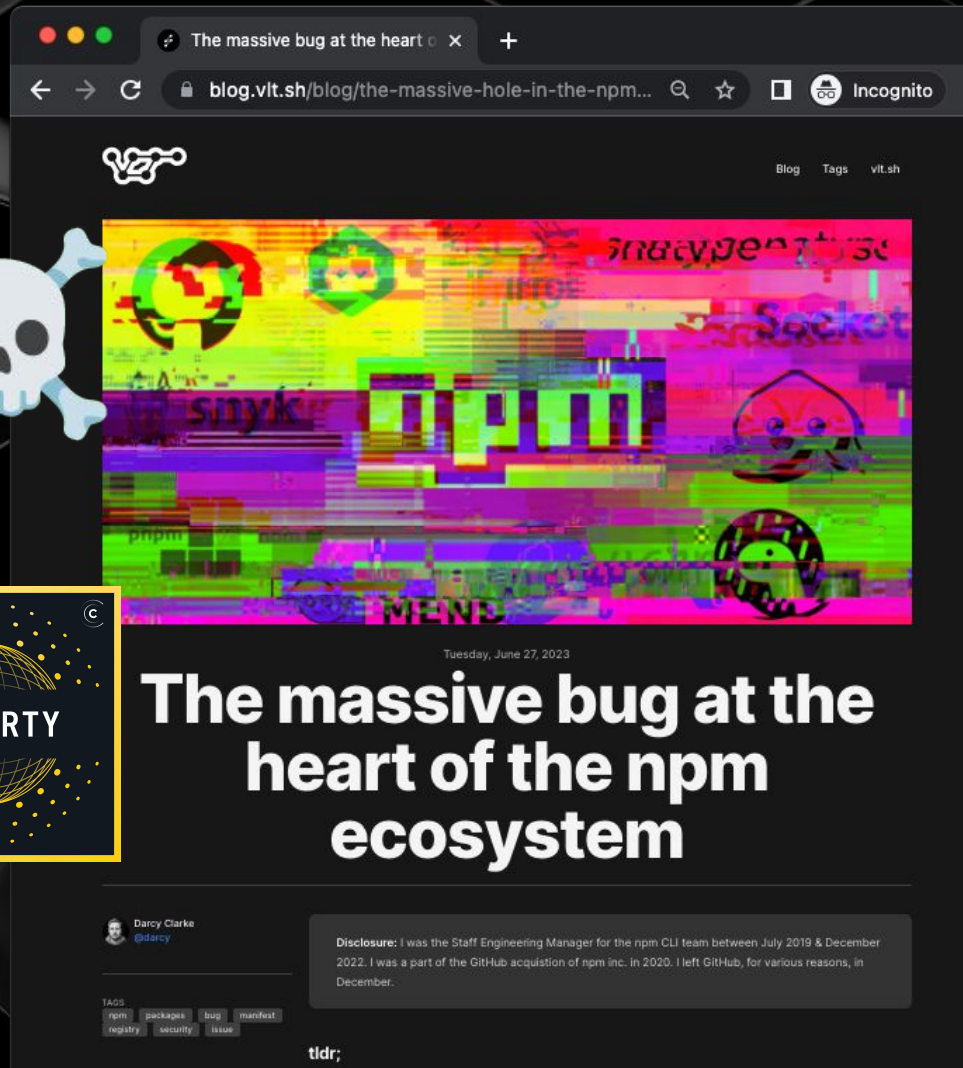
How can we mitigate

Manifest Confusion

- **Do not r**espect registry manifest data that is authored
- Use a **package's extracted package.json** as **the source of truth**

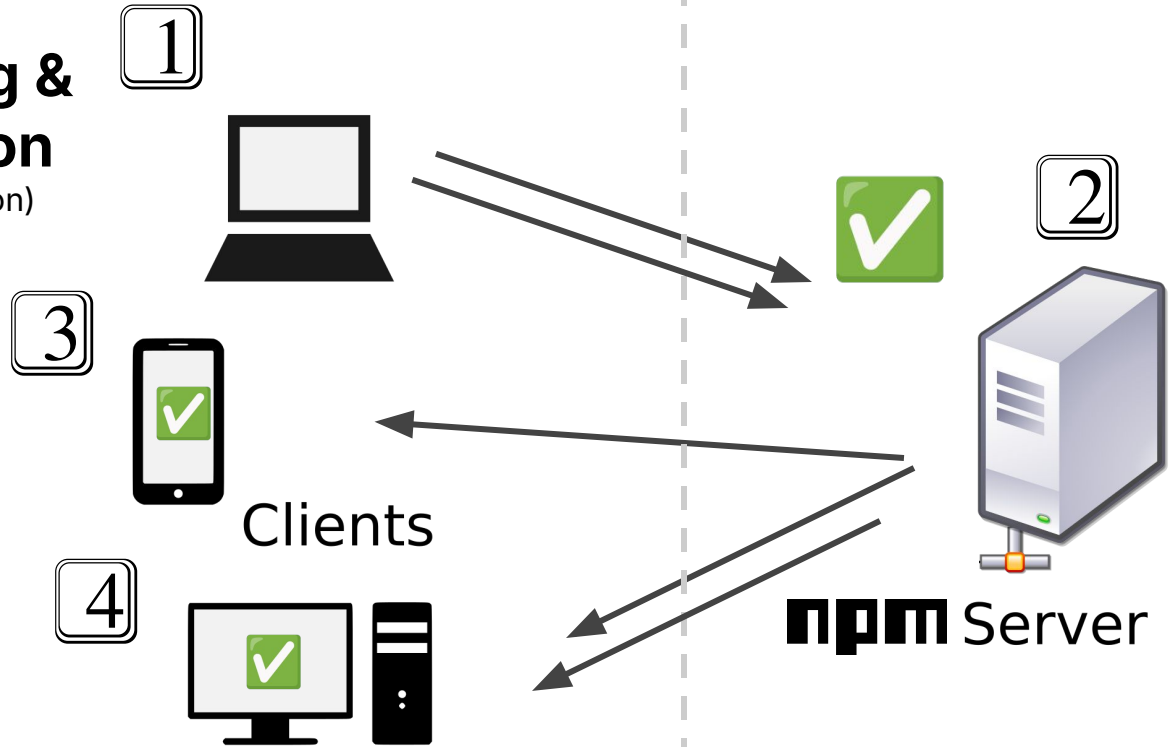
“is npm broken by design?”

https://**blog.vlt.sh**/blog/the-massive-hole-in-the-npm-ecosystem



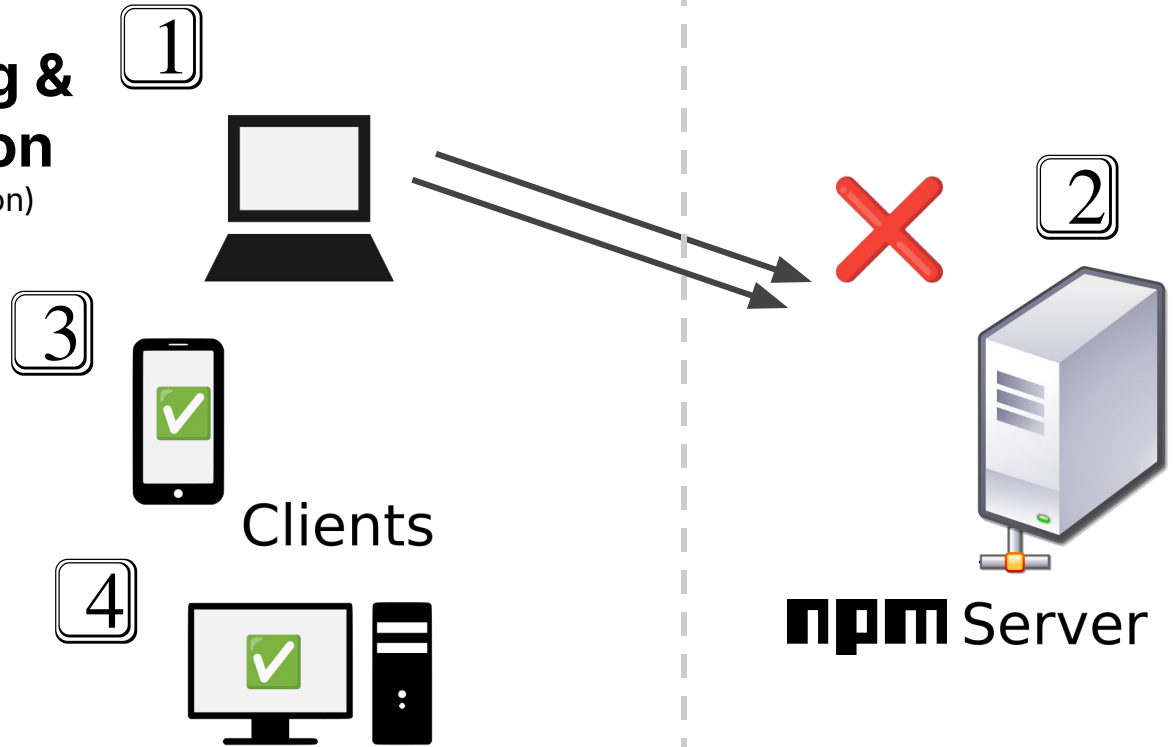
Package Publishing & Distribution

(Manifest Confusion)



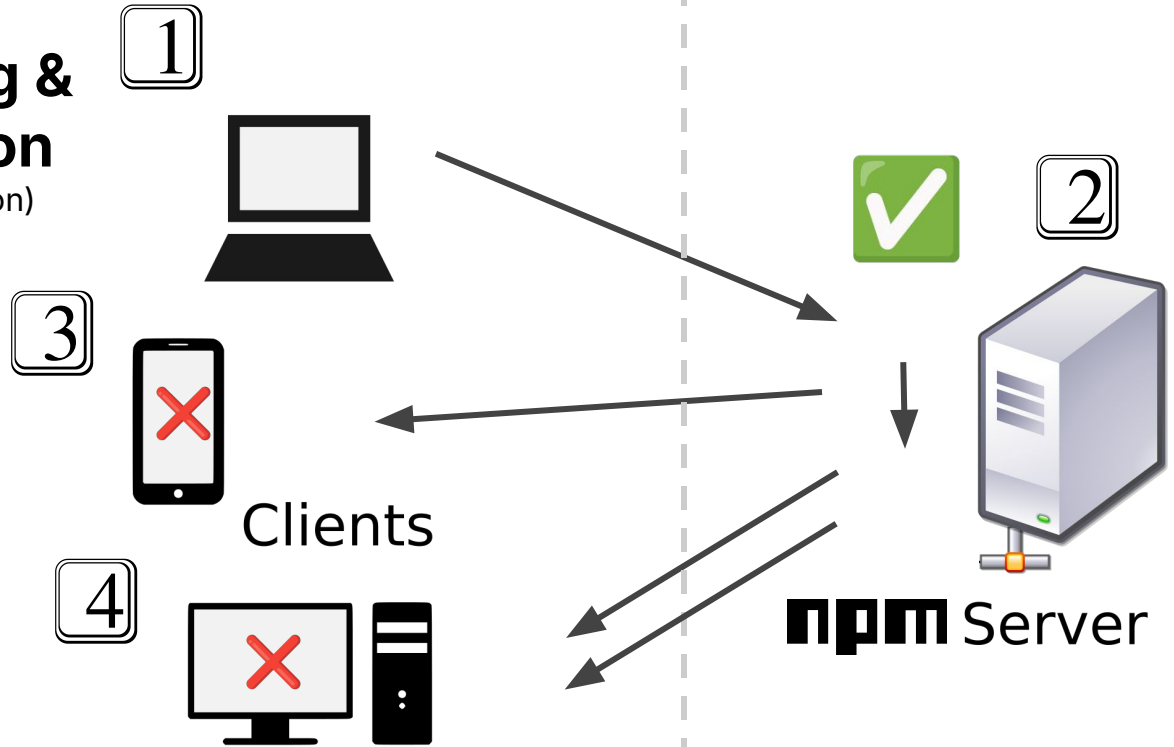
Package Publishing & Distribution

(Manifest Confusion)



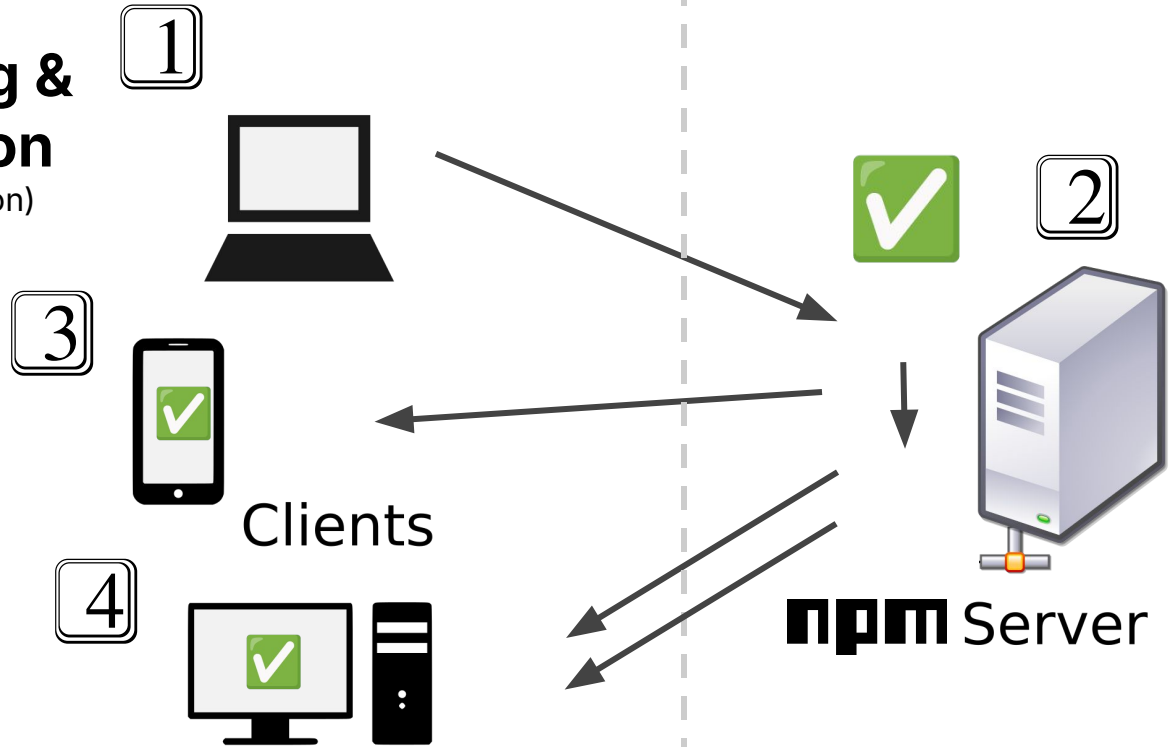
Package Publishing & Distribution

(Manifest Confusion)

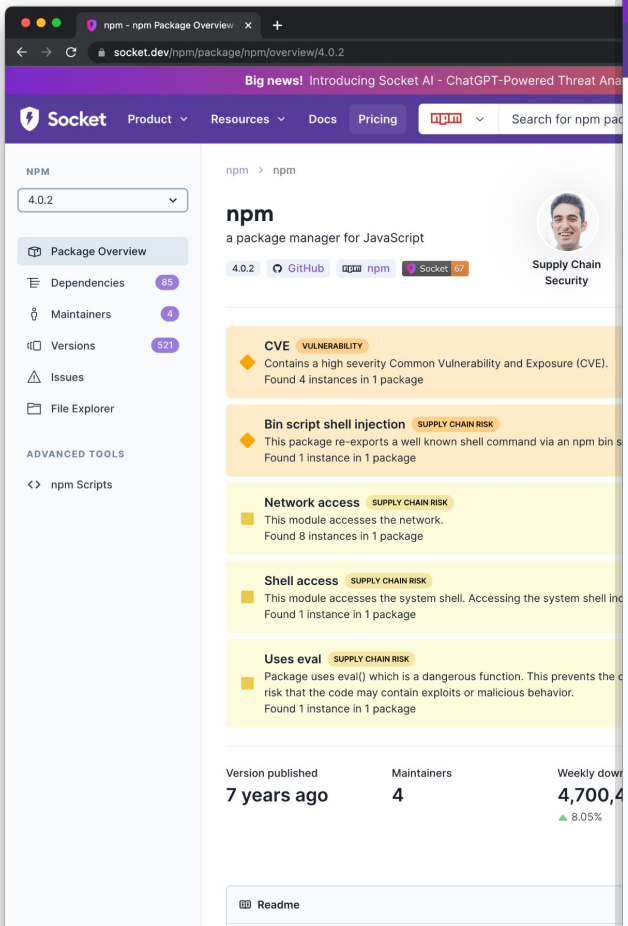


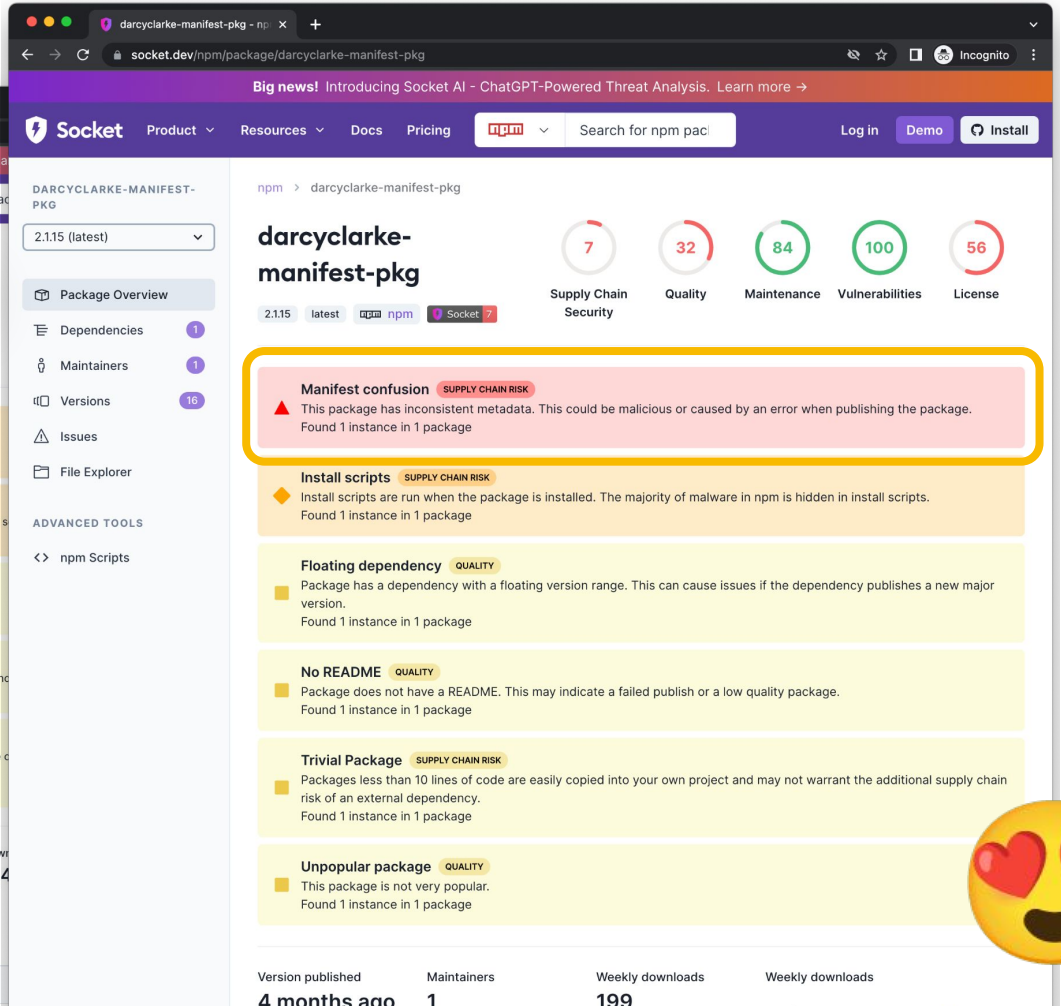
Package Publishing & Distribution

(Manifest Confusion)



socket.dev


npm - npm Package Overview
socket.dev/npm/package/npm/overview/4.0.2
Big news! Introducing Socket AI - ChatGPT-Powered Threat Ana
Socket
Product
Resources
Docs
Pricing
Search for npm pac
NPM
4.0.2
Package Overview
Dependencies 85
Maintainers 4
Versions 521
Issues
File Explorer
ADVANCED TOOLS
npm Scripts
npm › npm
npm
a package manager for JavaScript
4.0.2
GitHub
npm
Socket 67
Supply Chain Security
CVE VULNERABILITY
Contains a high severity Common Vulnerability and Exposure (CVE).
Found 4 instances in 1 package
Bin script shell injection SUPPLY CHAIN RISK
This package re-exports a well known shell command via an npm bin s
Found 1 instance in 1 package
Network access SUPPLY CHAIN RISK
This module accesses the network.
Found 8 instances in 1 package
Shell access SUPPLY CHAIN RISK
This module accesses the system shell. Accessing the system shell inc
Found 1 instance in 1 package
Uses eval SUPPLY CHAIN RISK
Package uses eval() which is a dangerous function. This prevents the c
risk that the code may contain exploits or malicious behavior.
Found 1 instance in 1 package
Version published
7 years ago
Maintainers
4
Weekly down
4,700,4
8.05%
Readme


darcyclarke-manifest-pkg - np
socket.dev/npm/package/darcyclarke-manifest-pkg
Incognito
Big news! Introducing Socket AI - ChatGPT-Powered Threat Analysis. Learn more →
Socket
Product
Resources
Docs
Pricing
Search for npm pac
Log in
Demo
Install
DARCYCLARKE-MANIFEST-PKG
2.1.15 (latest)
Package Overview
Dependencies 1
Maintainers 1
Versions 16
Issues
File Explorer
ADVANCED TOOLS
npm Scripts
npm › darcyclarke-manifest-pkg
darcyclarke-manifest-pkg
2.1.15
latest
npm
Socket 7
7
Supply Chain Security
32
Quality
84
Maintenance
100
Vulnerabilities
56
License
Manifest confusion SUPPLY CHAIN RISK
This package has inconsistent metadata. This could be malicious or caused by an error when publishing the package.
Found 1 instance in 1 package
Install scripts SUPPLY CHAIN RISK
Install scripts are run when the package is installed. The majority of malware in npm is hidden in install scripts.
Found 1 instance in 1 package
Floating dependency QUALITY
Package has a dependency with a floating version range. This can cause issues if the dependency publishes a new major version.
Found 1 instance in 1 package
No README QUALITY
Package does not have a README. This may indicate a failed publish or a low quality package.
Found 1 instance in 1 package
Trivial Package SUPPLY CHAIN RISK
Packages less than 10 lines of code are easily copied into your own project and may not warrant the additional supply chain risk of an external dependency.
Found 1 instance in 1 package
Unpopular package QUALITY
This package is not very popular.
Found 1 instance in 1 package
Version published
4 months ago
Maintainers
1
Weekly downloads
199
Weekly downloads

😍

How can we mitigate

Registry Compromise

- **Package Signing**
  - Packages published to npm are signed with a public key
  - Rotation of the key & new signatures were created in August 2022 using the ECDSA algorithm alongside new npm CLI validation
- **SSRI, Caching & Lockfiles**
- **Integrity Checks**

How can we mitigate

Account Takeovers

- **Mandatory Login Verification**
  Everyone - March 2022
- **Mandatory 2FA**
  Top-100 Maintainers - February 2022
  Top-500 Maintainers - May 2022
  High Impact - November 2022
- **Improved 2FA Experience**
  ex. Self-Serve Dashboard, Recovery Codes, Multiple Keys, Org-wide Management, WebAuthn
- **Improved Login Experience**
  ex. `npm login & npm publish (web login flow)`
- **Investments in Support & Authentication**
  ex. playbooks protecting against social engineering, identity verification & automation

High Impact Packages / Maintainers:
1 million+ weekly downloads or 500+ dependants

How can we mitigate

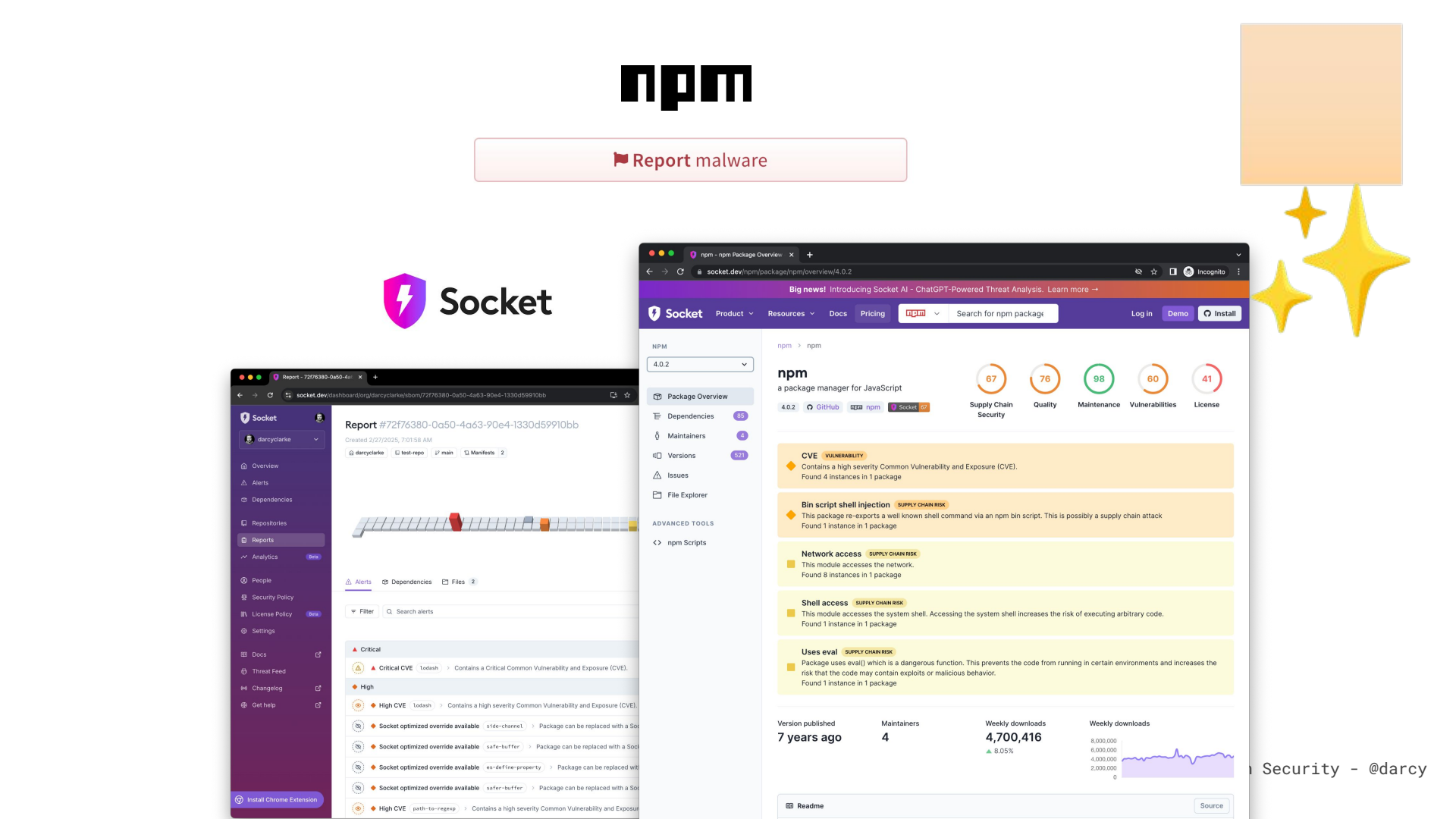
Malware

- **Focus on package contents**
- **Active scanning for known patterns**
  - AI models tracking behaviours
- **Automated takedowns/advisories**
  - Partnerships with security experts & reporting APIs

There are *other*

Threats

- **Noise**
- **Confusion**
- **Obfuscation**
- **Mutability**


Report malware
Socket
Report #72f76380-0a50-4a63-90e4-1330d59910bb
Socket
Product
Resources
Docs
Pricing
Search for npm package
Log in
Demo
Install
Big news! Introducing Socket AI - ChatGPT-Powered Threat Analysis. Learn more →
npm
a package manager for JavaScript
Supply Chain Security
Quality
Maintenance
Vulnerabilities
License
CVE
Bin script shell injection
Network access
Shell access
Uses eval
Version published
7 years ago
Maintainers
4
Weekly downloads
4,700,416
Readme
Source
Security - @darcy

Nondeterminism & Mutability

(ex. feature parity, remote third-party packages, install scripts etc.)

Example: **Create React App Project**

`package.json` post-initialization…

```
"dependencies": {
    "@testing-library/jest-dom": "^5.16.5",
    "@testing-library/react": "^13.4.0",
    "@testing-library/user-event": "^13.5.0",
    "react": "^18.2.0",
    "react-dom": "^18.2.0",
    "react-scripts": "5.0.1",
    "web-vitals": "^2.1.4"
}
```

ⓘ **7 Direct** Dependencies

Example:

Create React App Project

number of “**dependencies**” installed (no configuration)

yarn **v1**.22.19

1,256

pnpm **v7**.26.3

1,937

npm **v9**.4.2

1,408

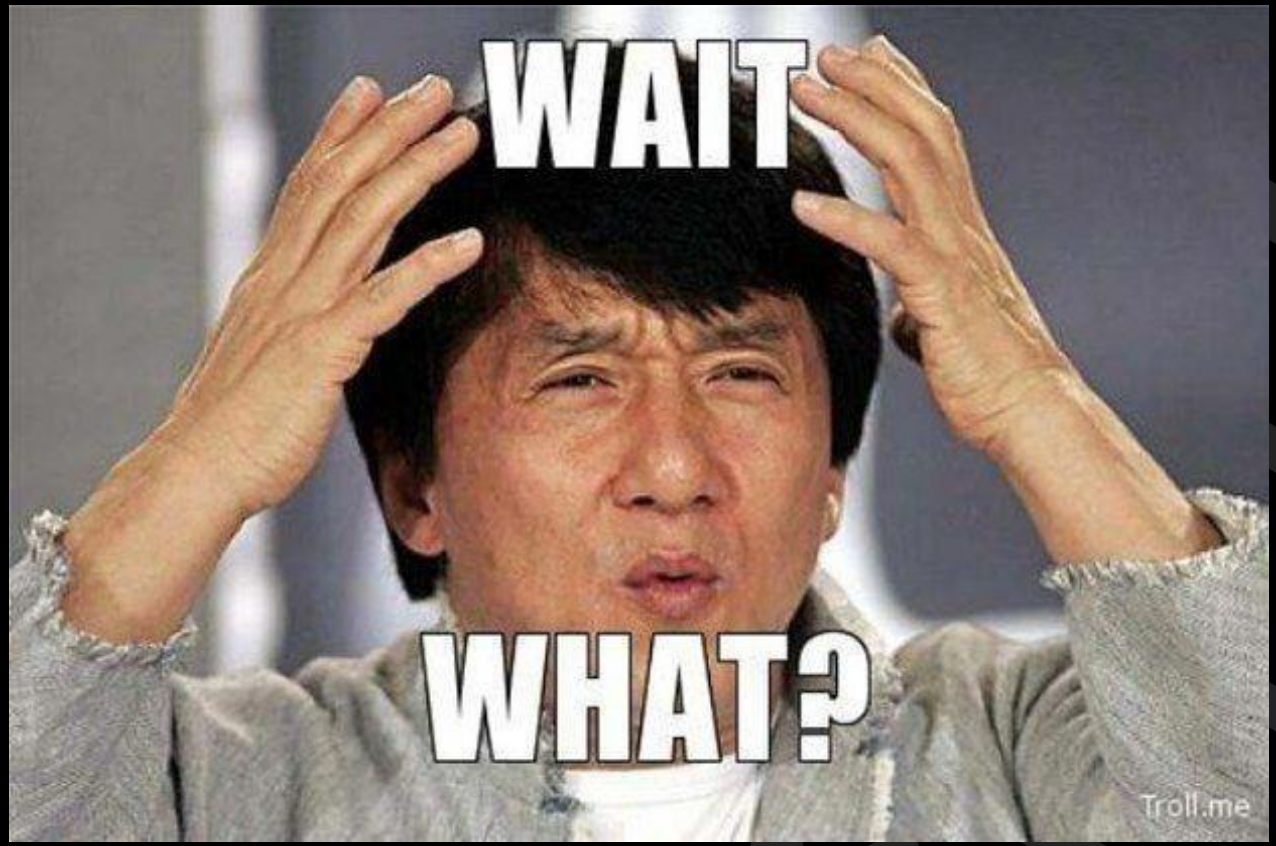
bun **v0**.5.5

1,386

deno **v1**.3.1

1,083

⚠ There is a **-+ ~850** diff in dependencies!


WAIT
WHAT?
Troll.me

Key:

Package managers treat these things (& more) differently...

Development Dependencies
Optional Dependencies (including environment-specific conditions)
Bundled Dependencies
Peer Dependencies
Overrides / Resolutions
Lifecycle **Scripts**


LIFE IS LIKE AN NPM INSTALL
YOU NEVER KNOW WHAT YOU'RE GONNA GET
imgflip.com

Avoid

Mutable Package References

- **Distribution Tags**
  ex. `"pkg@latest"`
- **Remote Tarball URLs**
  ex. `"https://example.com/file.tgz"`
  ex. `"https://example.com/"`
- **Remote Git Repository URLs**
  ex. `"https://github.com/user/repo.git"`
  ex. `"https://example.com/"`

⚠ Package Documents reference data that is both **mutable and immutable*** & package metadata **is not validated**

Use

Lockfiles

- Contains:
  - **Integrity Values (SSRI)**
  - **Resolved References**
  - **Tree Shape**

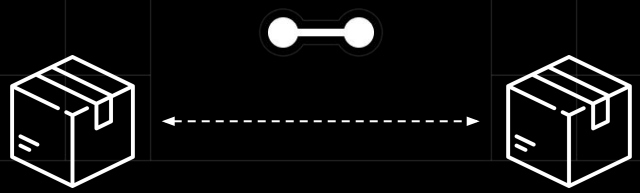
There is **hope**…

vlt /vōlt/

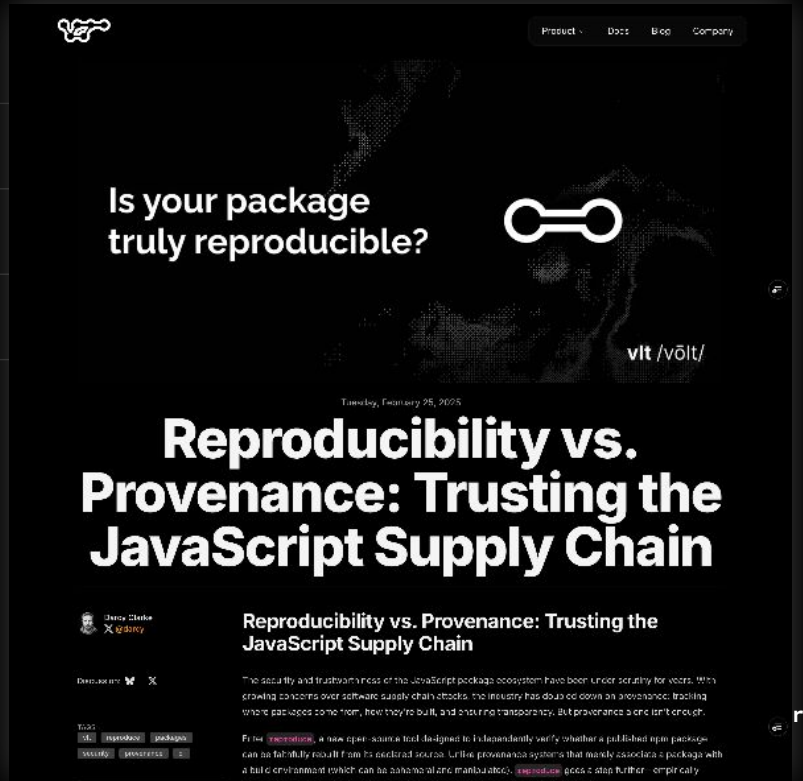
vlt.sh

Introducing “**reproduce**”

```
$ npx reproduce <pkg>
```



https://blog.vlt.sh/blog/**reproduce**



DSS
Dependency Selector Syntax

Dependency Selector Syntax (DSS)

https://docs.vlt.sh/packages/**query**

- CSS Selectors 4 Spec (syntax & operators)
- Answer complex, multi-faceted questions about dependencies, their relationships & associative metadata
- Consolidates redundant logic of similar, legacy list commands

Dependency Selector Syntax (DSS)

https://docs.vlt.sh/packages/**query**

```
*                           - all deps
:root > *                   - all direct deps
:root > .prod               - direct production deps
:root > .dev                - direct development deps
:root > * > .peer           - any peer dep of a direct deps
.workspace                  - any workspace dep
.workspace > .workspace     - all workspaces that depend on another workspace
.workspace:has(*.peer)      - all workspaces that have peer deps
[name=@vltpkg/query]        - deps named "@vltpkg/query"
#lodash                     - dep named "lodash"
#lodash[version~=1.2]       - deps named "lodash" & version starting w/ "1.2"
*:empty                     - deps with no other deps (ie. "leaf" nodes)
*:has(*)                    - has any deps
*:not(:empty)               - "" - equivalent to the above
*:type(git)                 - querying for all git dependencies
```

Dependency Selector Syntax (DSS)

https://docs.vlt.sh/packages/**query**

```
// find all dependencies with specific licenses
*[license="MIT"], *[license="ISC"]

// find all dependencies that have a node.engines property set
*:attr(engines,[node])

// find all dependencies that have defined react as an optional peer
*:has(#react):not(:attr(peerDependenciesMeta, react, [optional]))

// find all dependencies that have myself as a contributor
*:attr(contributors, [email=luke@lukekarrys.com])

// find all references to "install" scripts
*[scripts=install],
*[scripts=postinstall],
*[scripts=preinstall]
```

Dependency Selector Syntax (DSS)

https://docs.vlt.sh/packages/**query**

```
:semver(<spec>, <function>, <selector>) - semver comparator to [version]
```

- **spec** - a semver version or range
- **selector** - an attribute selector for each node (defaults to `[version]`)
- **functions** - a semver method to apply, one of: `satisfies`, `intersects`, `subset`, `gt`, `gte`, `gtr`, `lt`, `lte`, `ltr`, `eq`, `neq` or the special function `infer` (default `infer`)

```
:outdated          - have newer versions available
:outdated(<type>) - have a specific type of version available
                     ex. "MAJOR", "MINOR", "PATCH", defaults to "ANY"
```

Command Line

```
$ vlt query "<selector>"
```

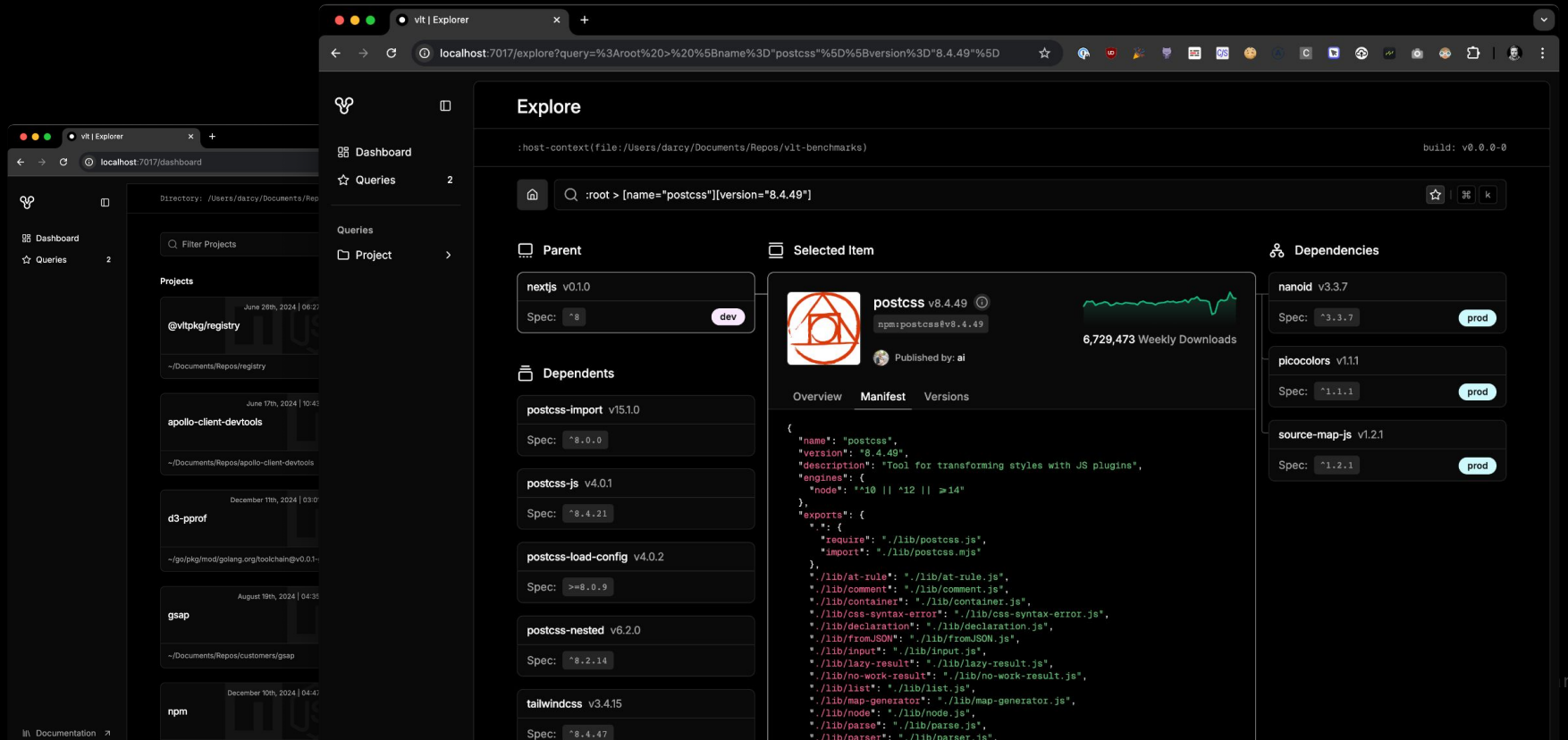
```
ex. vlt query "#react" | jq 'map(.name + "@" + .version)'
```

Programmatic Usage

`@vltpkg/query`

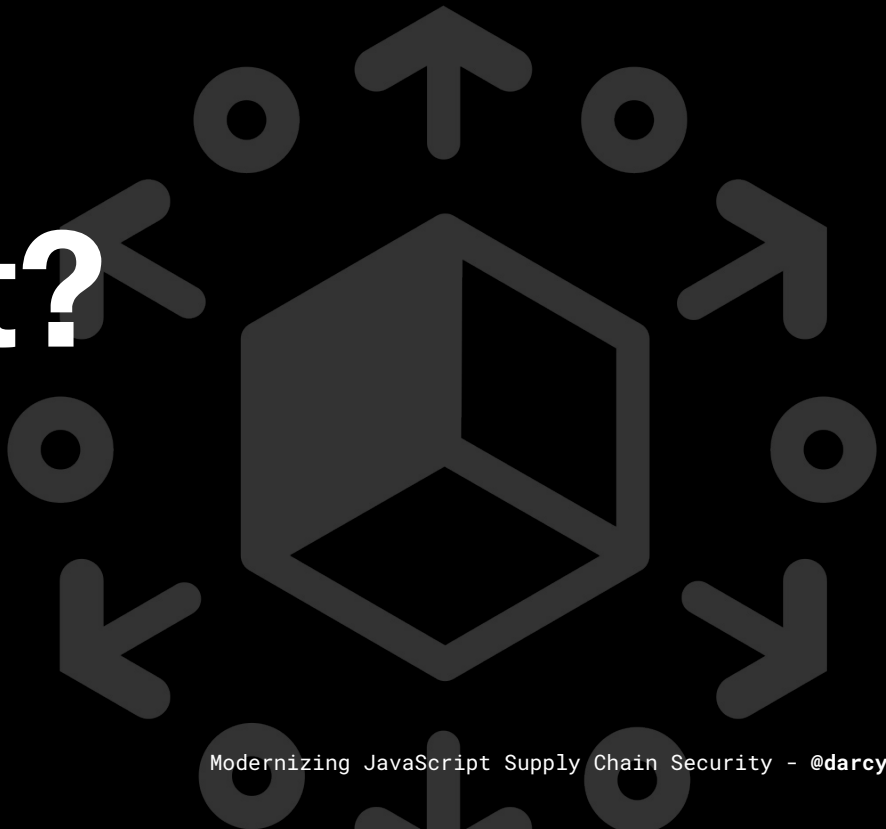
```
import { actual } from '@vltpkg/graph'
import { Query } from '@vltpkg/query'

const graph = await actual.load({ projectRoot: process.cwd() })
const query = new Query([...graph.nodes.values()])
query.search(':root > *')
```

GUI


vlt | Explorer
localhost:7017/explore?query=%3Aroot%20>%20%5Bname%3D"postcss"%5D%5Bversion%3D"8.4.49"%5D
Explore
Dashboard
Queries 2
Queries
Project
:host-context(file:/Users/darcy/Documents/Repos/vlt-benchmarks)
build: v0.0.0-0
:root > [name="postcss"][version="8.4.49"]
Parent
nextjs v0.1.0
Spec: ^8
dev
Selected Item
postcss v8.4.49
npm:postcss@v8.4.49
Published by: ai
6,729,473 Weekly Downloads
Overview
Manifest
Versions
{
"name": "postcss",
"version": "8.4.49",
"description": "Tool for transforming styles with JS plugins",
"engines": {
"node": "^10 || ^12 || >=14"
},
"exports": {
".": {
"require": "./lib/postcss.js",
"import": "./lib/postcss.mjs"
},
"./lib/at-rule": "./lib/at-rule.js",
"./lib/comment": "./lib/comment.js",
"./lib/container": "./lib/container.js",
"./lib/css-syntax-error": "./lib/css-syntax-error.js",
"./lib/declaration": "./lib/declaration.js",
"./lib/fromJSON": "./lib/fromJSON.js",
"./lib/input": "./lib/input.js",
"./lib/lazy-result": "./lib/lazy-result.js",
"./lib/no-work-result": "./lib/no-work-result.js",
"./lib/list": "./lib/list.js",
"./lib/map-generator": "./lib/map-generator.js",
"./lib/node": "./lib/node.js",
"./lib/parse": "./lib/parse.js",
"./lib/parser": "./lib/parser.js",
Dependencies
nanoid v3.3.7
Spec: ^3.3.7
prod
picocolors v1.1.1
Spec: ^1.1.1
prod
source-map-js v1.2.1
Spec: ^1.2.1
prod
Dependents
postcss-import v15.1.0
Spec: ^8.0.0
postcss-js v4.0.1
Spec: ^8.4.21
postcss-load-config v4.0.2
Spec: >=8.0.9
postcss-nested v6.2.0
Spec: ^8.2.14
tailwindcss v3.4.15
Spec: ^8.4.47
vlt | Explorer
localhost:7017/dashboard
Dashboard
Queries 2
Directory: /Users/darcy/Documents/Rep
Filter Projects
Projects
June 26th, 2024 | 06:27
@vltpkg/registry
~/Documents/Repos/registry
June 17th, 2024 | 10:43
apollo-client-devtools
~/Documents/Repos/apollo-client-devtools
December 11th, 2024 | 03:07
d3-pprof
~/go/pkg/mod/golang.org/toolchain@v0.0.1-
August 19th, 2024 | 04:35
gsap
~/Documents/Repos/customers/gsap
December 10th, 2024 | 04:47
npm
Documentation

Demo

What’s Next?



Security-Focused Pseudo States

```
:suspicious (ref. https://socket.dev/alerts/suspiciousStarActivity)
:undesirable (ref. https://socket.dev/alerts/troll)
:unstable (ref. https://socket.dev/alerts/unstableOwnership)
:abandoned (ref. https://socket.dev/alerts/missingAuthor)
:trivial (ref. https://socket.dev/alerts/trivialPackage)
:unknown (ref. https://socket.dev/alerts/newAuthor)
:unpopular (ref. https://socket.dev/alerts/unpopularPackage)
:deprecated (ref. https://socket.dev/alerts/deprecated)
:unmaintained (ref. https://socket.dev/alerts/unmaintained)
:shrinkwrap (ref. https://socket.dev/alerts/shrinkwrap)
:obfuscated (ref. https://socket.dev/alerts/obfuscatedFile)
:tracker (ref. https://socket.dev/alerts/telemetry)
:eval (ref. https://socket.dev/alerts/usesEval)
```

```
:scripts (ref. https://socket.dev/alerts/installScripts)
:shell (ref. https://socket.dev/alerts/shellAccess)
:native (ref. https://socket.dev/alerts/hasNativeCode)
:confused (ref. https://socket.dev/alerts/manifestConfusion)
:network (ref. https://socket.dev/alerts/networkAccess)
:debug (ref. https://socket.dev/alerts/debugAccess)
:dynamic (ref. https://socket.dev/alerts/dynamicRequire)
:fs (ref. https://socket.dev/alerts/filesystemAccess)
:entropic (ref. https://socket.dev/alerts/highEntropyStrings)
:env (ref. https://socket.dev/alerts/envVars)
:minified (ref. https://socket.dev/alerts/minifiedFile)
:deprecated (ref. https://socket.dev/alerts/deprecated)
```

Policies

package.json

```
"audit": {
    "policies": [
        {
            "name": "Vulnerable",
            "type": "error",
            "query": ":vulnerable"
        },
        {
            "name": "Peer Conflicts",
            "type": "error",
            "query": ".peer:not(:deduped)"
        },
        {
            "name": "Deprecated",
            "type": "warn",
            "query": ":deprecated"
        },
        ...
```

Shape:

```
{
  "name": "<name>",
  "type": "<log|warn|error>",
  "query": "<selector>"
}
```

Key Takeaways:

- **New tools** are here & more are coming soon…
- **Feature-rich** tools > fast tools
- Every new piece of **metadata** makes the **query language** & dep graph traversal more **powerful**
- **Accurate** information in supply chains is mission critical

Thank you!

Bluesky:
@darcyclarke.me

Twitter / X:
@darcy

GitHub:
@darcyclarke

Website:
darcyclarke.me

Bluesky:
@vltpkg.sh

Twitter / X:
@vltpkg

GitHub:
@vltpkg

Website:
vlt.sh

Please give feedback!