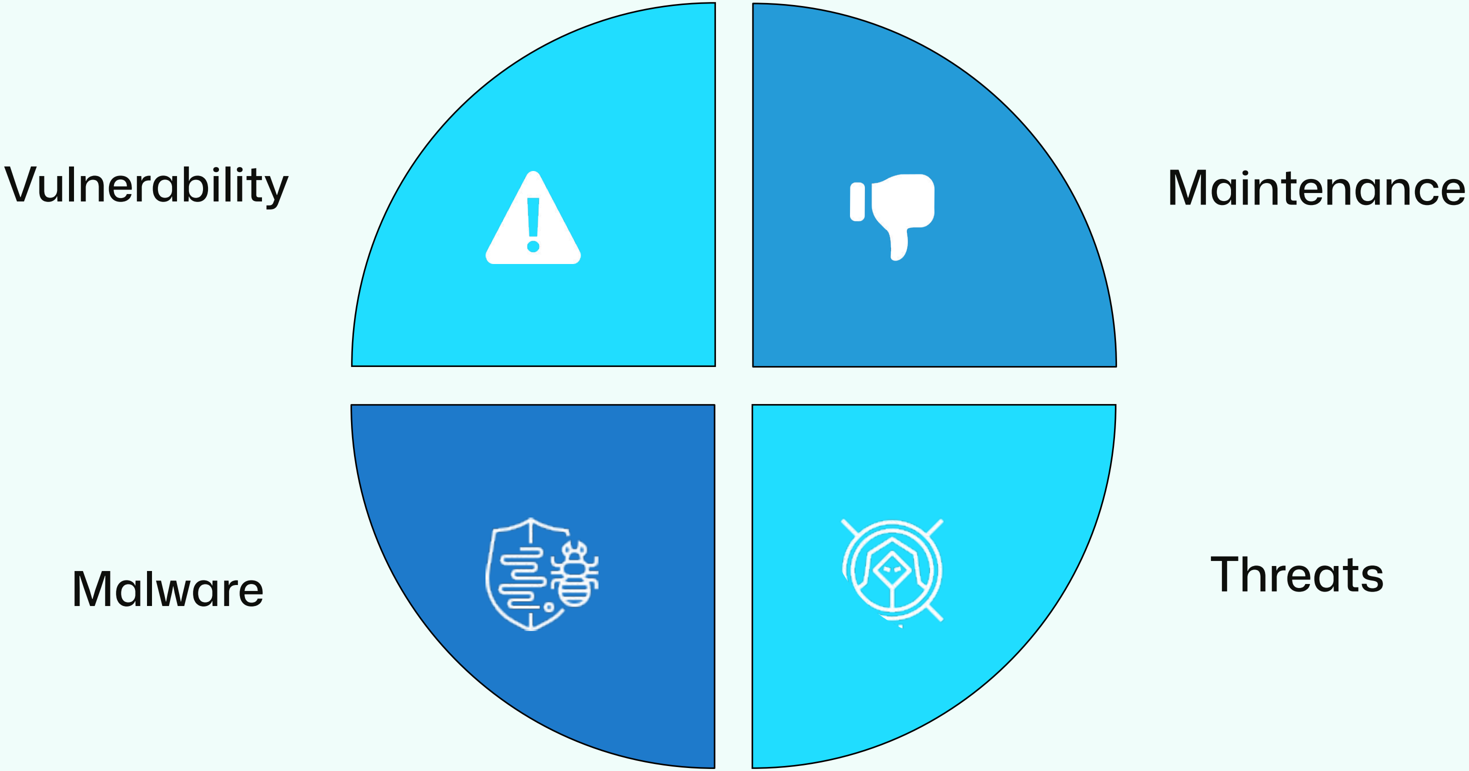
SafeDep

Guarding the Gates

Secure Open Source Library consumption with SafeDep vet

“Surprise! Most of what’s running in your codebase probably started as open source.

SO WHAT?



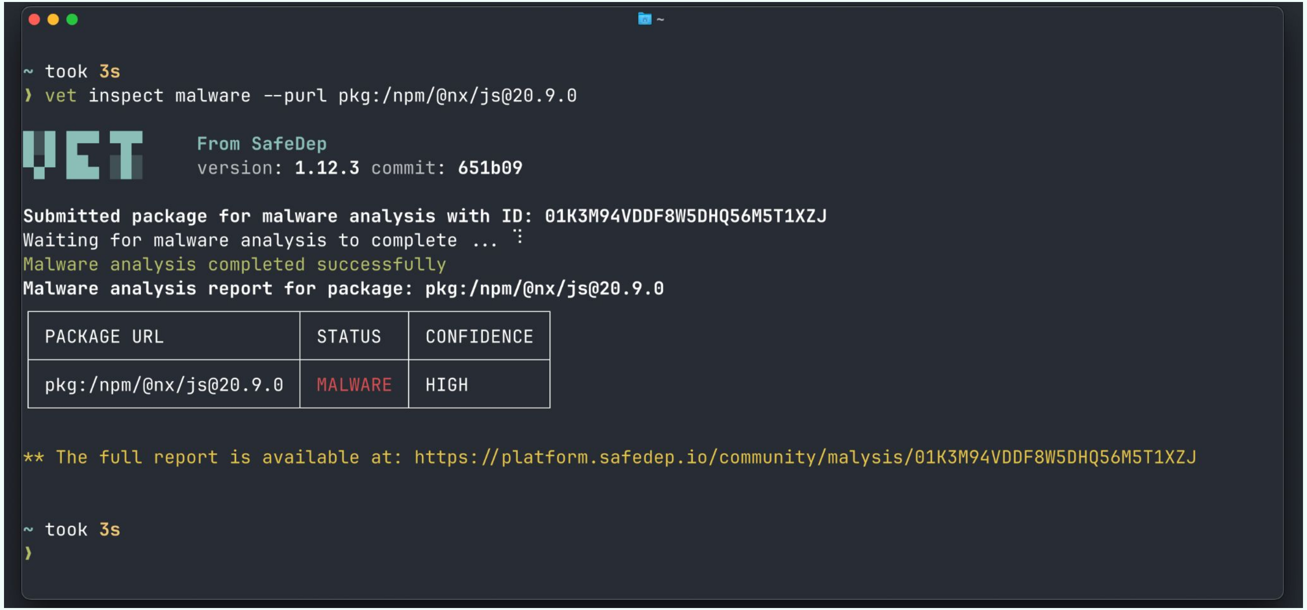
Some In Recent News

nx

6 MILLION

(Weekly downloads)

🔗 https://safedep.io/nx-build-system-compromise/

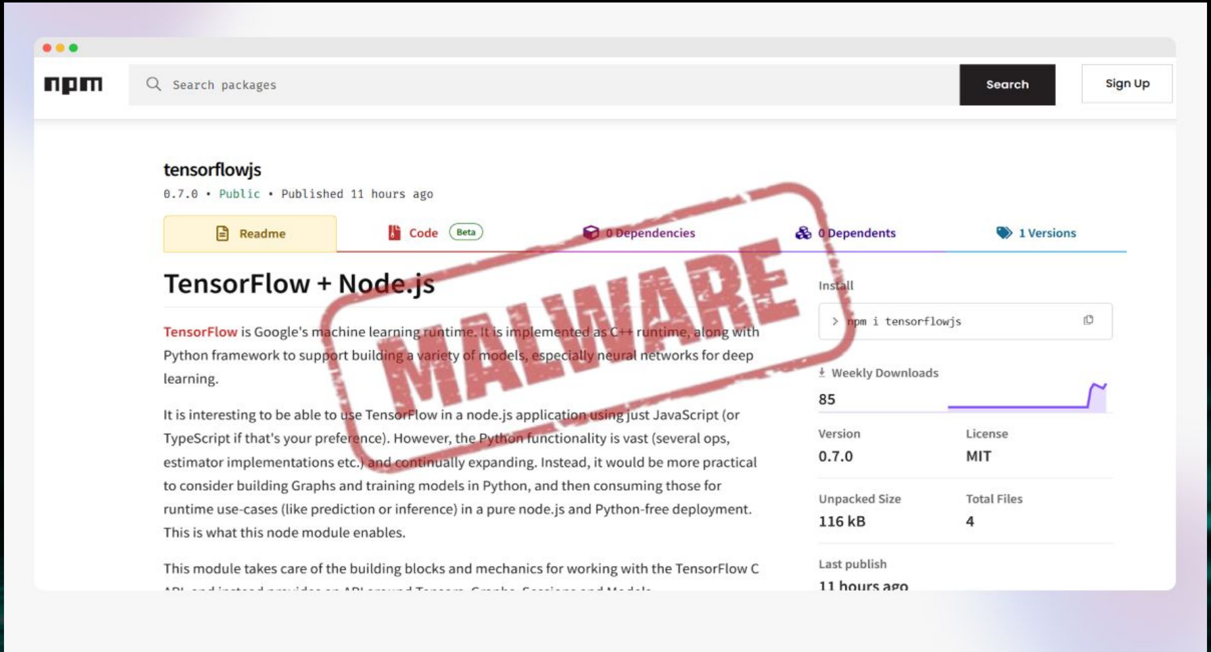


```
~ took 3s
❯ vet inspect malware --purl pkg:/npm/@nx/js@20.9.0

                From SafeDep
                version: 1.12.3 commit: 651b09

Submitted package for malware analysis with ID: 01K3M94VDDF8W5DHQ56M5T1XZJ
Waiting for malware analysis to complete ... ⠸
Malware analysis completed successfully
Malware analysis report for package: pkg:/npm/@nx/js@20.9.0
┌───────────────────────┬─────────┬────────────┐
│ PACKAGE URL           │ STATUS  │ CONFIDENCE │
├───────────────────────┼─────────┼────────────┤
│ pkg:/npm/@nx/js@20.9.0│ MALWARE │ HIGH       │
└───────────────────────┴─────────┴────────────┘

** The full report is available at: https://platform.safedep.io/community/malysis/01K3M94VDDF8W5DHQ56M5T1XZJ


~ took 3s
❯
```

SafeDep

@tensorflowjs **Typosquatting attack**

safedep.io/http://malicious-npm-package-targeting-tensorflow-users/



tensorflowjs

0.7.0 • Public • Published 11 hours ago

TensorFlow + Node.js

TensorFlow is Google's machine learning runtime. It is implemented as C++ runtime, along with Python framework to support building a variety of models, especially neural networks for deep learning.

It is interesting to be able to use TensorFlow in a node.js application using just JavaScript (or TypeScript if that's your preference). However, the Python functionality is vast (several ops, estimator implementations etc.) and continually expanding. Instead, it would be more practical to consider building Graphs and training models in Python, and then consuming those for runtime use-cases (like prediction or inference) in a pure node.js and Python-free deployment. This is what this node module enables.

This module takes care of the building blocks and mechanics for working with the TensorFlow C API, and instead provides an API around Tensors, Graphs, Sessions and Models

Install

```
> npm i tensorflowjs
```

Weekly Downloads

85

Version	License
0.7.0	MIT

Unpacked Size	Total Files
116 kB	4

Last publish

11 hours ago

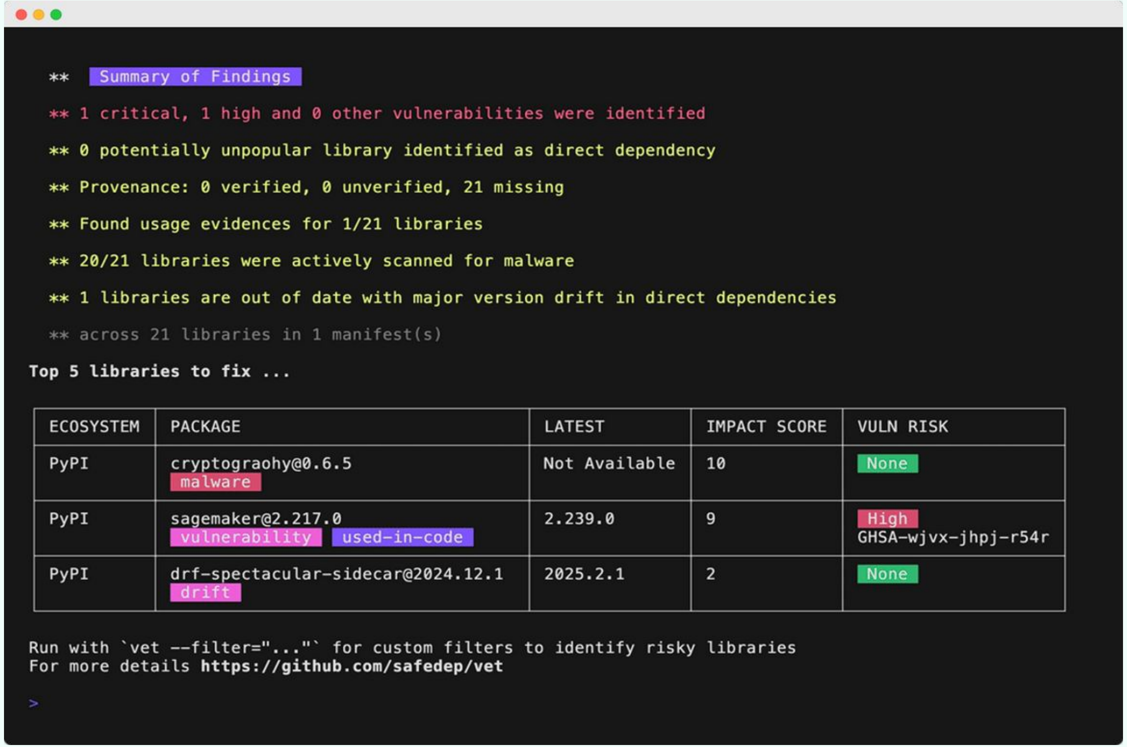
What Should we do?

Skip FOSS

Don’t skip open source-just outsmart the risks

Introducing vet

vet is an open source tool that protects your software supply chain by detecting vulnerabilities and malicious packages across major ecosystems like npm, PyPI, Maven, Go, Docker, and GitHub Actions.

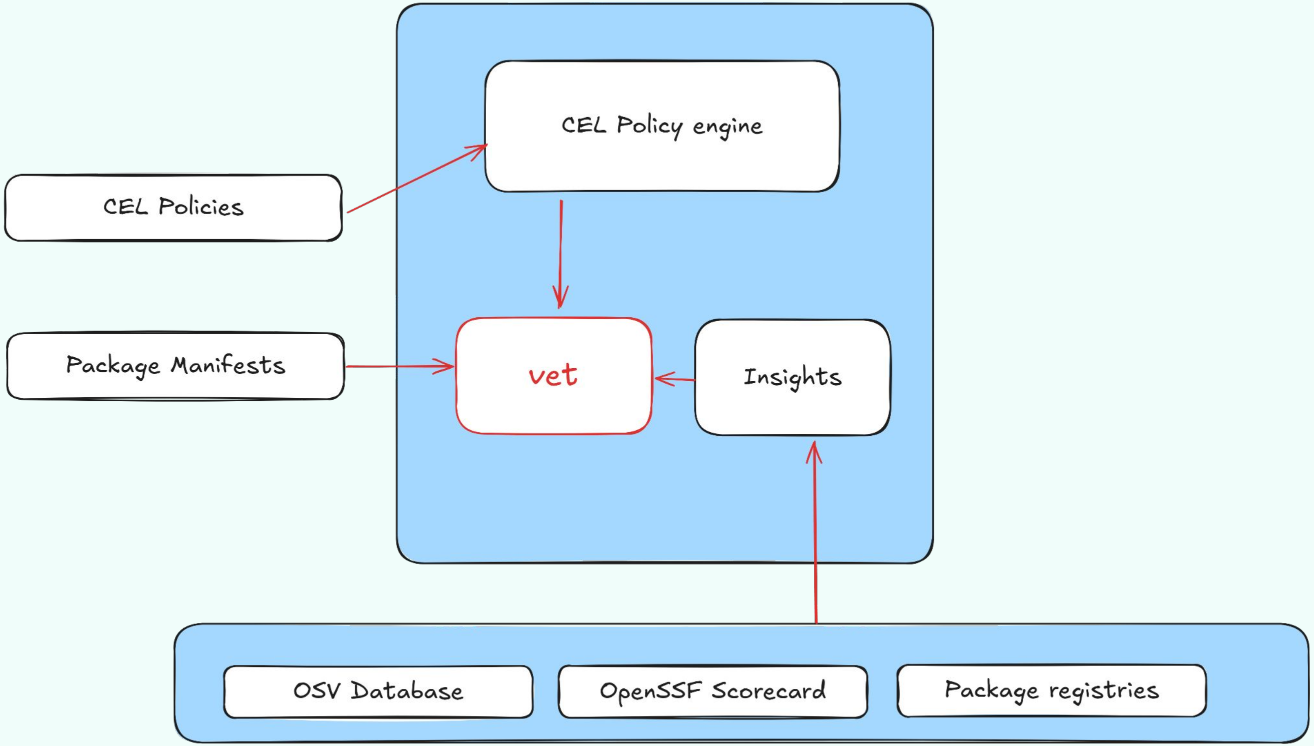


```
  **  Summary of Findings
  ** 1 critical, 1 high and 0 other vulnerabilities were identified
  ** 0 potentially unpopular library identified as direct dependency
  ** Provenance: 0 verified, 0 unverified, 21 missing
  ** Found usage evidences for 1/21 libraries
  ** 20/21 libraries were actively scanned for malware
  ** 1 libraries are out of date with major version drift in direct dependencies
  ** across 21 libraries in 1 manifest(s)
Top 5 libraries to fix ...

 | ECOSYSTEM | PACKAGE                                | LATEST        | IMPACT SCORE | VULN RISK           |
 | PyPI      | cryptograohy@0.6.5                     | Not Available | 10           | None                |
 |           |  malware                               |               |              |                     |
 | PyPI      | sagemaker@2.217.0                      | 2.239.0       | 9            | High                |
 |           |  vulnerability   used-in-code          |               |              | GHSA-wjvx-jhpj-r54r |
 | PyPI      | drf-spectacular-sidecar@2024.12.1      | 2025.2.1      | 2            | None                |
 |           |  drift                                 |               |              |                     |

Run with `vet --filter="..."` for custom filters to identify risky libraries
For more details https://github.com/safedep/vet

>
```

github.com/safedep/vet

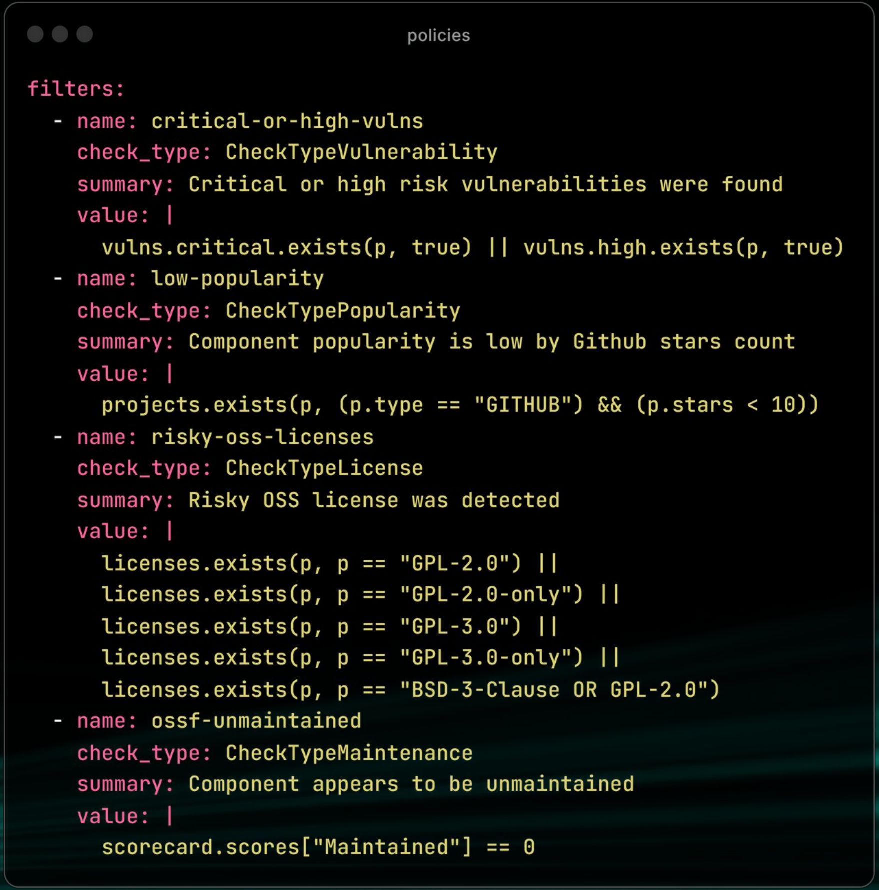
SafeDep

How vet works



What Are These Policies?

Define security policies using CEL expressions to enforce context specific security requirements.

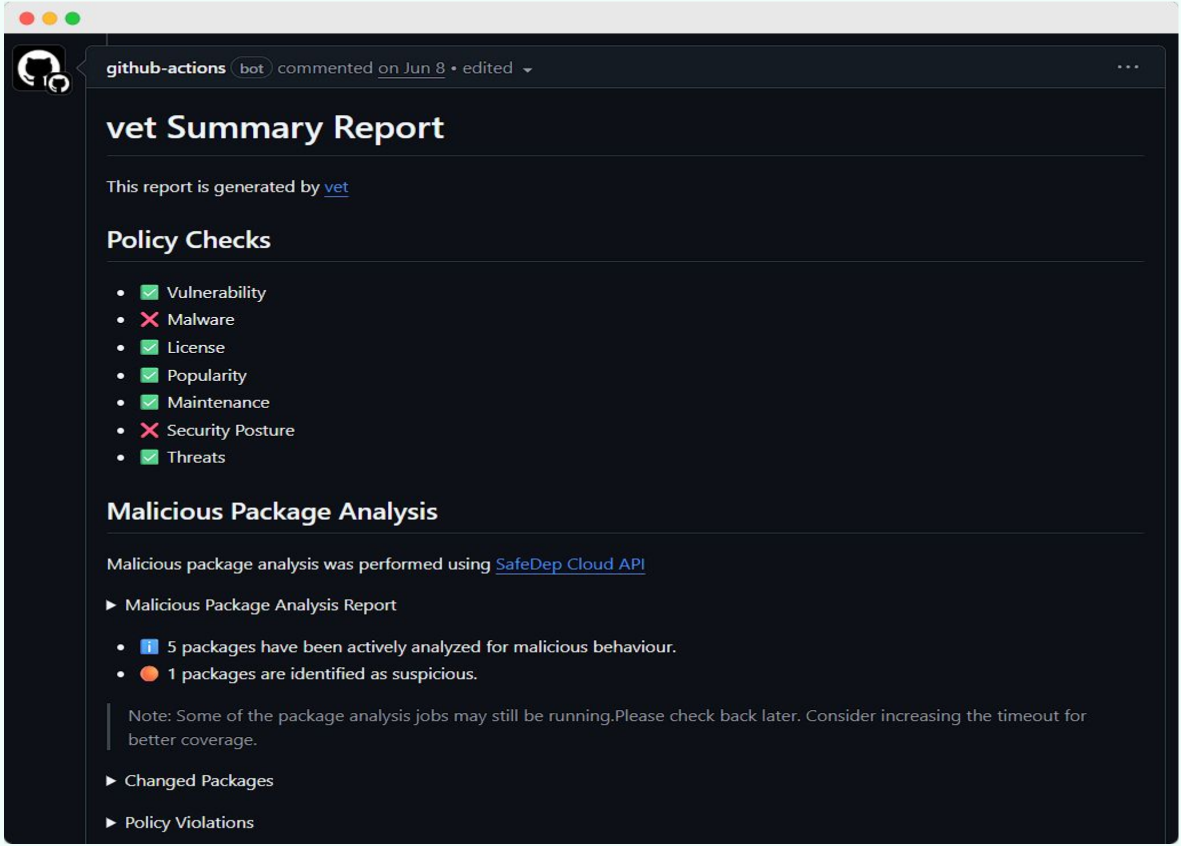


```
filters:
  - name: critical-or-high-vulns
    check_type: CheckTypeVulnerability
    summary: Critical or high risk vulnerabilities were found
    value: |
      vulns.critical.exists(p, true) || vulns.high.exists(p, true)
  - name: low-popularity
    check_type: CheckTypePopularity
    summary: 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
```

SafeDep

vet in action

vet FOSS in CI/CD using Policy as Code



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

- ℹ️ 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.

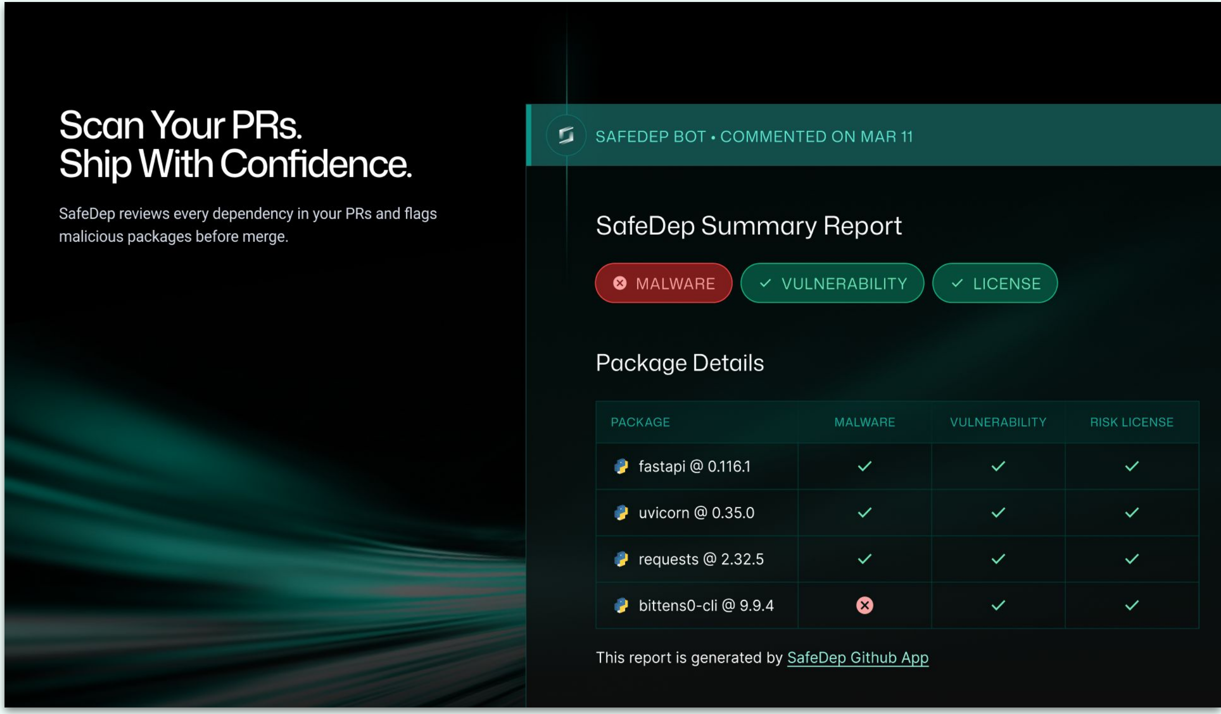
▶ Changed Packages

▶ Policy Violations

🔗 github.com/safedep/vet-action

SafeDep

Use SafeDep Github App to manage your open source software supply chain



Scan Your PRs.
Ship With Confidence.

SafeDep reviews every dependency in your PRs and flags malicious packages before merge.

SAFEDEP BOT • COMMENTED ON MAR 11

SafeDep Summary Report

☒ MALWARE ✓ VULNERABILITY ✓ LICENSE

Package Details

PACKAGE	MALWARE	VULNERABILITY	RISK LICENSE
fastapi @ 0.116.1	✓	✓	✓
uvicorn @ 0.35.0	✓	✓	✓
requests @ 2.32.5	✓	✓	✓
bittens0-cli @ 9.9.4	☒	✓	✓

This report is generated by SafeDep Github App

docs.safedep.io/apps/github

SafeDep

How many more ways vet can help?

01 vet supports native GitLab Dependency Scanning.

02 vet supports container scanning for images

03 With PMG, vet proactively blocks malicious packages as developers install dependencies

Become a part of vet community

★ github.com/safedep/vet

01 You can contribute to code

02 Help writing documentation

03 Report Bugs

SafeDep

About Me

Sudhanshu Dasgupta

Software Engineer, SafeDep Inc

github.com/sudhanshutech

linkedin.com/in/sudhanshu-dasgupta

SafeDep

Thank You

Ship Code.
Not Malware.

SafeDep