SAFEDEP

Surfing the Wild Wild West of Open Source Software Supply Chain Attacks

Abhisek Datta

https://safedep.io

Agenda

1. What is **risky** Open Source?
2. **Hands-on:** Automated Open Source package vetting using `vet`
3. Hacking on `vet`: Contributing to Open Source security tools
4. Build your own tool(s)

SAFEDEP

Who uses Open Source Software (code)?

Hint: Every software development team in the world, including you & me!

Entrepreneurship

Open Source Software: The $9 Trillion Resource Companies Take for Granted

Many companies build their businesses on open source software, code that would cost firms $8.8 trillion to create from scratch if it weren't freely available. Research by **Frank Nagle** and colleagues puts a value on an economic necessity that will require investment to meet demand.

Featuring Frank Nagle and Manuel Hoffmann. By Rachel Layne on March 22, 2024.

Harvard Business School

SAFEDEP

Case Study: Critical Vulnerability Inherited from OSS

CVE-2022-47966 - Unauthenticated remote code execution in Zoho Manage Engine

caused by

Apache Santuario (xmlsec) component which fails to properly validate XML signatures of SAML responses received during the authentication flow

https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html

SAFEDEP

Open Source Threat Landscape Today

SECURITY CRYPTOCURRENCY MALWARE

Ultralytics AI Library with 60M Downloads Compromised for Cryptomining

Lottie Player compromised in supply chain attack – all you need to know

CVE-2024-3094 The targeted backdoor supply chain attack against XZ and liblzma

2024 in Open Source Malware Report

Sonatype has identified 778,529 pieces of open source malware. Explore the trends and insights from our research.

North Korea malware on npm and Ledger connect-kit crypto heist

Researchers Find Over 22,000 Removed PyPI Packages at Risk of Revival Hijack

Sep 04, 2024 Ravie Lakshmanan

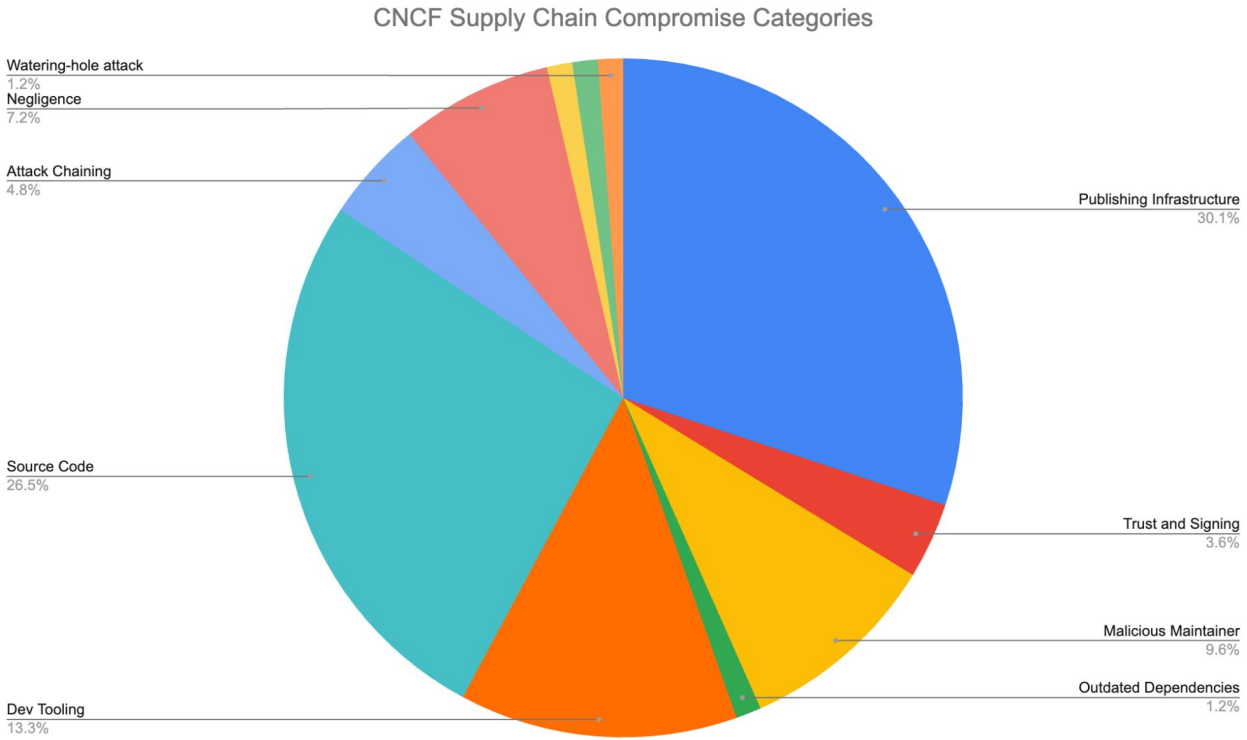
SAFEDEP

https://safedep.io/malicious-oss-package-analysis-llm-oracle/
https://www.sonatype.com/blog/lottie-player-compromised-in-supply-chain-attack-all-you-need-to-know

Case Study: Reverse Engineering llm-oracle npm Malware

https://safedep.io/malicious-oss-package-analysis-llm-oracle/

Software Composition Analysis (SCA) ?



Find vulnerable Open Source dependencies by matching library versions with proprietary and public vulnerability databases.

SCA

SAFEDEP

Categorization of REAL WORLD Software Supply Chain Security Incidents

https://safedep.io/why-oss-risks-larger-than-sca/

Introducing vet

Open source tool, written in Go, for policy (as code) driven vetting of open source software components in CI/CD

+ more ..

github.com/safedep/vet

SAFEDEP

Installing `vet`

- Install using Homebrew
  - **brew tap safedep/tap**
  - **brew install safedep/tap/vet**
- Alternatively, download and install pre-compiled binary from GitHub

https://github.com/safedep/vet/releases

Getting Started

- Download the binary file for your operating system / architecture from the Official GitHub Releases
- You can also install `vet` using homebrew in MacOS and Linux

```
brew tap safedep/tap
brew install safedep/tap/vet
```

- Alternatively, build from source

> Ensure $(go env GOPATH)/bin is in your $PATH

```
go install github.com/safedep/vet@latest
```

- Also available as a container image

```
docker run --rm -it ghcr.io/safedep/vet:latest version
```

> **Note:** Container image is built for x86_64 Linux only. Use a pre-built binary or build from source for other platforms.

https://github.com/safedep/vet

SAFEDEP

Alternative - Try in your browser

- Alternative to installation
- Limited usage
- Limited alternative

https://killercoda.com/abhisek/scenario/101-intro

SAFEDEP

The Playground

```
$ git clone \
https://github.com/safedep/demo-client-python demo-app
```

```
$ cd ./demo-app
```

All examples in the workshop **slides** will use this *intentionally* vulnerable app. Feel free to scan your own code base!

SAFEDEP

Sneak Peak: Running your 1st `vet` scan

`vet scan`

- Other scan options
  - `vet scan -M requirements.txt`
  - `vet scan -M go.mod`
  - `vet scan -M package-lock.json`
  - `vet scan --purl pkg:/npm/express@4.17.1`

```
❯ vet scan -D demo-client-java
Scanning packages    ... done! [115 in 12.715s]
Scanning manifests   ... done! [1 in 12.715s]
  **  Summary of Findings

  ** 1 critical, 5 high and 5 other vulnerabilities were identified

  ** 1 potentially unpopular library identified as direct dependency

  ** 78 libraries are out of date with major version drift in direct dependencies

  ** across 115 libraries in 1 manifest(s)

Consider upgrading the following libraries for maximum impact:
```

PACKAGE	UPDATE TO	IMPACT
org.yaml:snakeyaml@1.30 vulnerability drift	2.0	13
org.springframework.security:spring-security-core@5.7.3 vulnerability drift	6.0.2	7
com.sun.istack:istack-commons-runtime@3.0.12 low popularity drift	4.1.1	4
com.fasterxml.jackson.core:jackson-databind@2.13.4 vulnerability	2.14.2	3
commons-fileupload:commons-fileupload@1.4 vulnerability	1.5	3

```
There are 77 more libraries that should be upgraded to reduce risk
Run vet with `--report-markdown=/path/to/report.md` for details

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

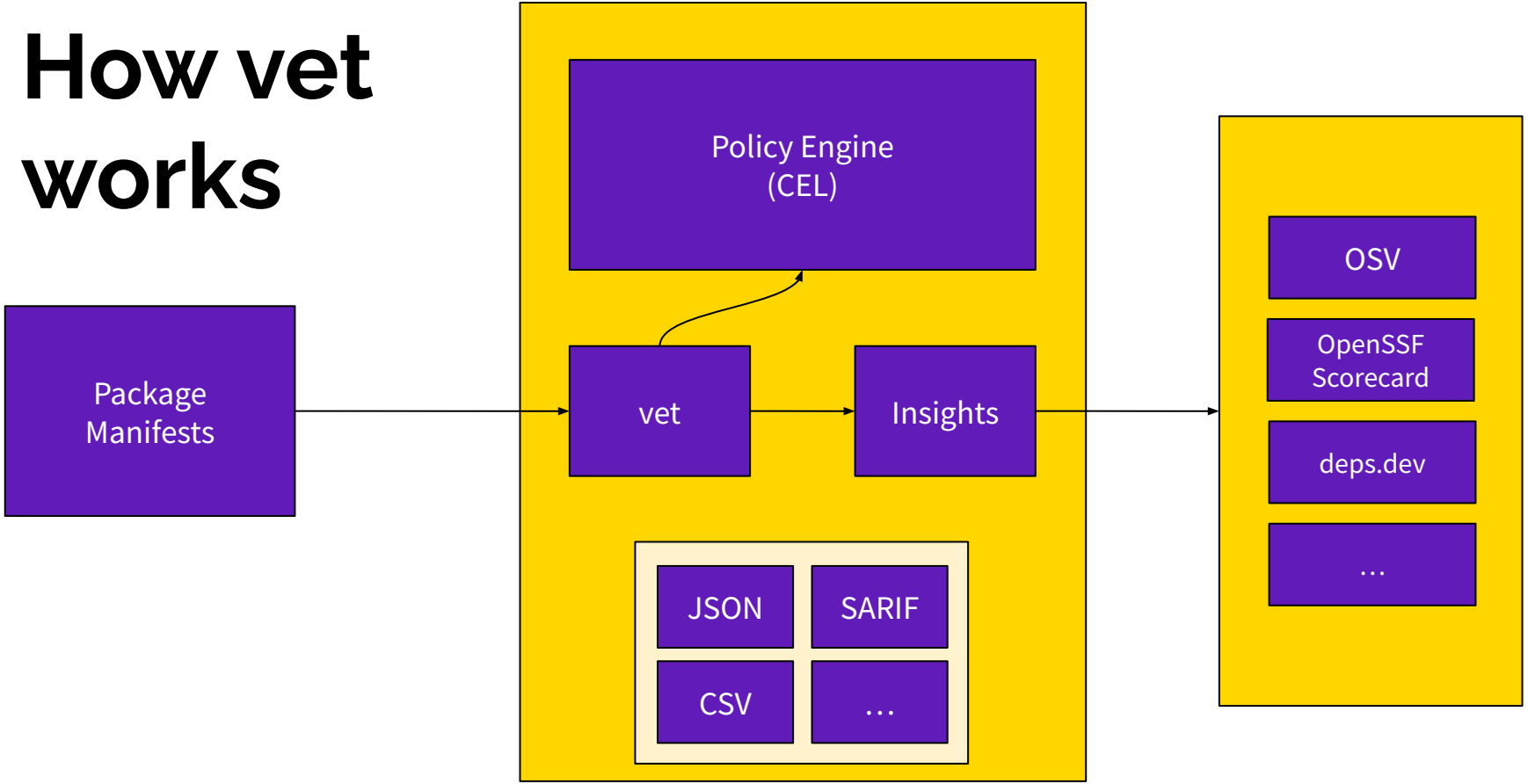
SAFEDEP

What we will do with `vet` TODAY?

1. Run `vet` locally with policy, query, reporting & more
2. Setup `vet-action` with GitHub Action (CI/CD) as a security guardrail
3. Setup `vet` for malicious package scanning
4. Enable `vet-action` to perform malicious package scanning in CI/CD
5. Hacking `vet`

SAFEDEP

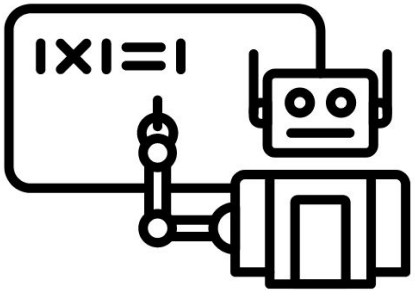
How vet works



SAFEDEP

vet Policies are CEL

Common Expressions Language




```
vulns.critical.
size() > 0
```

vet OSS package for vulnerabilities

SAFEDEP

Preparing for Local Policy Query

- Start by running `vet scan` to create a local cache of JSON data to query using *Policy as Code*

```
vet scan --transitive \
  --json-dump-dir /tmp/vet-json
```

SAFEDEP

Using `vet` Policy as Code

```
vet query --from /tmp/vet-json \
    --filter 'vulns.critical.size() > 0'
```

```
vet query --from /tmp/vet-json \
    --filter 'vulns.critical.size() > 0'
```

```
vet query --from /tmp/vet-json \
    --filter 'scorecard.scores.Maintained == 0'
```

SAFEDEP

https://docs.safedep.io/advanced/filtering

Generating Reports

```
vet query --from /tmp/vet-json \
  --report-json report.json
```

```
vet query --from /tmp/vet-json \
  --filter 'vulns.critical.size() > 0 || vulns.high.size() > 0' \
  --report-csv report.csv
```

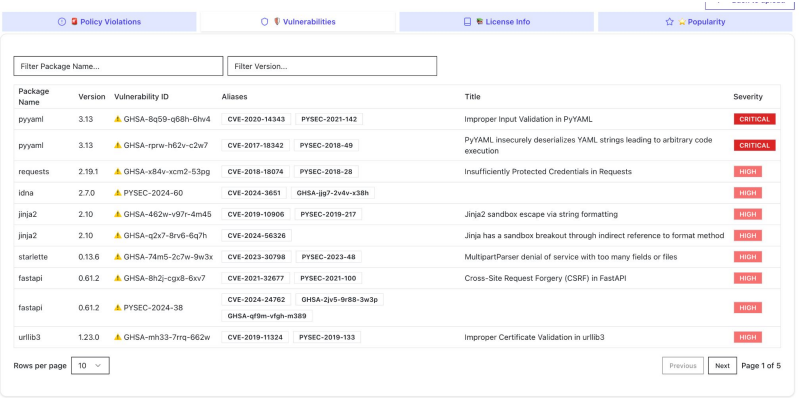
SAFEDEP

`vet` supports other reporting formats. See `vet` query -h

Visualizing Report (JSON)

🚀 `vet` JSON reports can be visualized using

`https://vetpkg.dev/vr`



SAFEDEP

Dependency Usage Evidence using Code Analysis

Analyze source code and build database

```
vet code scan \
   --db code.db
```

Run vet scan with code analysis enabled

```
vet scan \
   --code code.db
```

ECOSYSTEM	PACKAGE	LATEST	IMPACT SCORE	VULN RISK
PyPI	jinja2@2.10 vulnerability drift used-in-code	3.1.5	25	High GHSA-462w-v97r-4m45 + 1
PyPI	pyyaml@3.13 vulnerability drift	6.0.2	22	Critical GHSA-8q59-q68h-6hv4 + 1
PyPI	fastapi@0.61.2 vulnerability used-in-code	0.115.9	17	High GHSA-8h2j-cgx8-6xv7 + 1
PyPI	requests@2.19.1 vulnerability used-in-code	2.32.3	13	High GHSA-x84v-xcm2-53pg
PyPI	uvicorn@0.11.7 used-in-code	0.34.0	1	None

https://youtu.be/yFUuMMAsnfI?feature=shared

SAFEDEP

Malicious Package Scanning using `vet`

1. Malicious Package Scanning is an **optional** SafeDep Cloud service
2. Register with SafeDep Cloud to obtain Tenant Domain and API Key
3. Run `vet` to execute malicious package scanning

SAFEDEP

Register `vet` to use SafeDep Cloud API

`vet cloud quickstart`

- Requires free sign-up / login
- Creates tenant
- Creates API key
- Configure credentials in vet config

```
➜  vet git:(feat/cloud-quickstart) ✗ vet cloud quickstart

Yb    dP 888888 888888
 Yb  dP  88__     88
  YbdP   88""     88
   YP    888888   88

🚀 Starting SafeDep Cloud Quickstart...
👋 Hello! Let's get you onboarded..
🔑 Start by creating an account or sign-in to your existing account
Please visit https://auth.safedep.io/activate?user_code=VZMZ-RNVL and enter
✅ Successfully authenticated you!
🔑 Saving your cloud credentials in your local config...
✅ Successfully saved your cloud credentials!
🔍 Checking if you have an existing tenant...
^[📝 Looks like you don't have an existing tenant. Let's create one for you
? 👤 What should we call you? John Doe
? 📝 We have automatically generated a domain for you. Here is your chance
✅ Successfully created a new tenant!
🔑 Please wait while we get you onboarded...
```

https://youtu.be/ykSiP547xuA

SAFEDEP

Using `vet` to Scan for Malicious Packages

```
export VET_ENABLE_PACKAGE_INSPECT_COMMAND=true
```

```
vet inspect malware \
   --purl pkg:/npm/chrome-api-utils@1.1.0
```

SAFEDEP

Using vet to Scan for Malicious Packages

```
→  vet git:(main) vet inspect malware --purl pkg:/npm/postcss-optimizer@3.2.7

Yb    dP 888888 888888
 Yb  dP  88__     88
  YbdP   88""     88
   YP    888888   88

Submitted package for malware analysis with ID: 01JK7D3466VTBBDDGERQJ1HVXR
Waiting for malware analysis to complete ... ⠹
Malware analysis completed successfully
Malware analysis report for package: pkg:/npm/postcss-optimizer@3.2.7
```

PACKAGE URL	STATUS	CONFIDENCE
pkg:/npm/postcss-optimizer@3.2.7	MALWARE	UNSPECIFIED

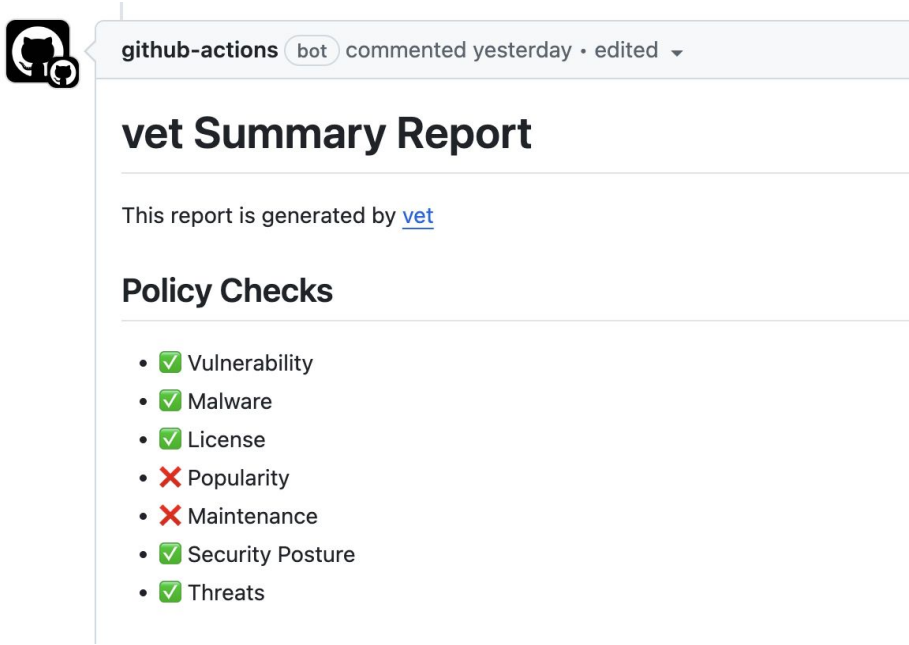
```
** The full report is available at: https://platform.safedep.io/community/malysis/01JK7D3466VTBBDDGERQJ1HVXR

→  vet git:(main)
```

SAFEDEP

vet as Proactive Security Guardrails with GitHub

1. Navigate to https://github.com/safedep/demo-client-python
2. Fork the repository
3. Clone your fork & switch to a dev branch
4. Follow instructions at https://github.com/safedep/vet-action to integration vet in your forked repository
5. Create pull request to main branch of your forked repository from your dev branch



SAFEDEP

Hacking `vet`

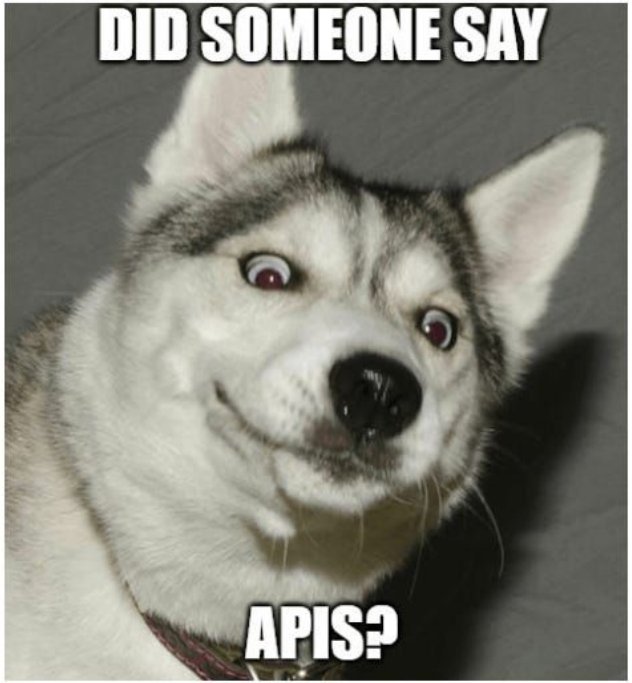
1. What is it to contribute to an OSS project?
2. How to contribute?
    a. Look at issues, bugs or work on new feature
    b. Fork the repository at https://github.com/safedep/vet
    c. Push your changes to your forked repository
    d. Raise pull request to the upstream repository
    e. Get your pull request reviewed by a maintainer
    f. Congratulations 🎉You are now an OSS contributor!

SAFEDEP

Build Your Own Tools (BYOT 🎉)

API

https://github.com/safedep/api-examples



SAFEDEP

Build Your Own Tools

1. Package Insights
2. Malicious Package Analysis
3. Consolidated SBOM & Query

SAFEDEP

Thank You!

@abh1sek

github.com/abhisek

github.com/safedep/vet

SAFEDEP