Secure Consumption of Open Source Software: Evaluating, Utilizing, and Contributing Safely

Katherine Druckman
Open Source Security Evangelist
Why are we here?

Today we’ll cover

- Security challenges in consuming open source software
- Evaluating open source projects through a security lens
- Project health, governance, management, and community
- Tools for securing open source software
- Open source community security efforts: OpenSSF
- How we can contribute to a safer ecosystem
Why is open source security so challenging?
Open source is everywhere

- 96% of codebases
- 77% of code within
- 70–90% of all software

Source: Synopsys
Source: Linux Foundation

https://www.linuxfoundation.org/blog/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on
Open source is everywhere

Yay! We won!
Millions of packages ...
Millions of packages ... dozens of maintainers

Packages by number of maintainers

Bulk of projects have a single maintainer

https://anchore.com/blog/open-source-is-bigger-than-you-imagine/
It’s not just NPM

<table>
<thead>
<tr>
<th>Registry</th>
<th>Packages</th>
<th>Versions</th>
<th>Maintainers</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>npmjs.org</td>
<td>3,639,251</td>
<td>41,815,290</td>
<td>822,231</td>
<td>742,169</td>
</tr>
<tr>
<td></td>
<td>41,815,290</td>
<td>822,231</td>
<td>742,169</td>
<td>70,056</td>
</tr>
<tr>
<td></td>
<td>3,639,251</td>
<td>41,815,290</td>
<td>822,231</td>
<td>742,169</td>
</tr>
<tr>
<td></td>
<td>3,639,251</td>
<td>41,815,290</td>
<td>822,231</td>
<td>742,169</td>
</tr>
<tr>
<td></td>
<td>3,639,251</td>
<td>41,815,290</td>
<td>822,231</td>
<td>742,169</td>
</tr>
<tr>
<td></td>
<td>3,639,251</td>
<td>41,815,290</td>
<td>822,231</td>
<td>742,169</td>
</tr>
<tr>
<td></td>
<td>3,639,251</td>
<td>41,815,290</td>
<td>822,231</td>
<td>742,169</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Registry</th>
<th>Packages</th>
<th>Versions</th>
<th>Maintainers</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>proxy.golang.org</td>
<td>1,105,378</td>
<td>9,970,233</td>
<td>449,953</td>
<td>70,056</td>
</tr>
<tr>
<td></td>
<td>1,105,378</td>
<td>9,970,233</td>
<td>449,953</td>
<td>70,056</td>
</tr>
<tr>
<td></td>
<td>1,105,378</td>
<td>9,970,233</td>
<td>449,953</td>
<td>70,056</td>
</tr>
<tr>
<td></td>
<td>1,105,378</td>
<td>9,970,233</td>
<td>449,953</td>
<td>70,056</td>
</tr>
<tr>
<td></td>
<td>1,105,378</td>
<td>9,970,233</td>
<td>449,953</td>
<td>70,056</td>
</tr>
<tr>
<td></td>
<td>1,105,378</td>
<td>9,970,233</td>
<td>449,953</td>
<td>70,056</td>
</tr>
<tr>
<td></td>
<td>1,105,378</td>
<td>9,970,233</td>
<td>449,953</td>
<td>70,056</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Registry</th>
<th>Packages</th>
<th>Versions</th>
<th>Maintainers</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>hub.docker.com</td>
<td>1,001,771</td>
<td>10,844,967</td>
<td>411,451</td>
<td>1,713</td>
</tr>
<tr>
<td></td>
<td>1,001,771</td>
<td>10,844,967</td>
<td>411,451</td>
<td>1,713</td>
</tr>
<tr>
<td></td>
<td>1,001,771</td>
<td>10,844,967</td>
<td>411,451</td>
<td>1,713</td>
</tr>
<tr>
<td></td>
<td>1,001,771</td>
<td>10,844,967</td>
<td>411,451</td>
<td>1,713</td>
</tr>
<tr>
<td></td>
<td>1,001,771</td>
<td>10,844,967</td>
<td>411,451</td>
<td>1,713</td>
</tr>
<tr>
<td></td>
<td>1,001,771</td>
<td>10,844,967</td>
<td>411,451</td>
<td>1,713</td>
</tr>
<tr>
<td></td>
<td>1,001,771</td>
<td>10,844,967</td>
<td>411,451</td>
<td>1,713</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Registry</th>
<th>Packages</th>
<th>Versions</th>
<th>Maintainers</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>nuget.org</td>
<td>624,254</td>
<td>7,566,455</td>
<td>85,940</td>
<td>129,237</td>
</tr>
<tr>
<td></td>
<td>624,254</td>
<td>7,566,455</td>
<td>85,940</td>
<td>129,237</td>
</tr>
<tr>
<td></td>
<td>624,254</td>
<td>7,566,455</td>
<td>85,940</td>
<td>129,237</td>
</tr>
<tr>
<td></td>
<td>624,254</td>
<td>7,566,455</td>
<td>85,940</td>
<td>129,237</td>
</tr>
<tr>
<td></td>
<td>624,254</td>
<td>7,566,455</td>
<td>85,940</td>
<td>129,237</td>
</tr>
<tr>
<td></td>
<td>624,254</td>
<td>7,566,455</td>
<td>85,940</td>
<td>129,237</td>
</tr>
<tr>
<td></td>
<td>624,254</td>
<td>7,566,455</td>
<td>85,940</td>
<td>129,237</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Registry</th>
<th>Packages</th>
<th>Versions</th>
<th>Maintainers</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>pypi.org</td>
<td>542,396</td>
<td>5,603,074</td>
<td>229,691</td>
<td>193,748</td>
</tr>
<tr>
<td></td>
<td>542,396</td>
<td>5,603,074</td>
<td>229,691</td>
<td>193,748</td>
</tr>
<tr>
<td></td>
<td>542,396</td>
<td>5,603,074</td>
<td>229,691</td>
<td>193,748</td>
</tr>
<tr>
<td></td>
<td>542,396</td>
<td>5,603,074</td>
<td>229,691</td>
<td>193,748</td>
</tr>
<tr>
<td></td>
<td>542,396</td>
<td>5,603,074</td>
<td>229,691</td>
<td>193,748</td>
</tr>
<tr>
<td></td>
<td>542,396</td>
<td>5,603,074</td>
<td>229,691</td>
<td>193,748</td>
</tr>
<tr>
<td></td>
<td>542,396</td>
<td>5,603,074</td>
<td>229,691</td>
<td>193,748</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Registry</th>
<th>Packages</th>
<th>Versions</th>
<th>Maintainers</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>repo1.maven.org</td>
<td>499,556</td>
<td>11,361,001</td>
<td>66,310</td>
<td>31,287</td>
</tr>
<tr>
<td></td>
<td>499,556</td>
<td>11,361,001</td>
<td>66,310</td>
<td>31,287</td>
</tr>
<tr>
<td></td>
<td>499,556</td>
<td>11,361,001</td>
<td>66,310</td>
<td>31,287</td>
</tr>
<tr>
<td></td>
<td>499,556</td>
<td>11,361,001</td>
<td>66,310</td>
<td>31,287</td>
</tr>
<tr>
<td></td>
<td>499,556</td>
<td>11,361,001</td>
<td>66,310</td>
<td>31,287</td>
</tr>
<tr>
<td></td>
<td>499,556</td>
<td>11,361,001</td>
<td>66,310</td>
<td>31,287</td>
</tr>
<tr>
<td></td>
<td>499,556</td>
<td>11,361,001</td>
<td>66,310</td>
<td>31,287</td>
</tr>
</tbody>
</table>

---

Statistics:

- Registries: 59
- Packages: 8,840,726
- Versions: 97,334,410
- Namespaces: 1,328,127
- Maintainers: 1,440,484
- Downloads: 1,811,443,044,372
- Keywords: 1,521,288

https://ecosyste.ms
Common Vulnerabilities and Exposures (CVE)

CVE is a dictionary of common names for publicly known cybersecurity vulnerabilities, each of which receives a CVE Identifier.

CVE Identifiers make it easy to share data across separate network security databases and tools. Plus, they provide a baseline for evaluating the coverage of an organization’s security tools.

- CVE = Common Vulnerabilities and Exposures
- List of “all” publicly known software security vulnerabilities starting in 1999
- MITRE Corporation manages and maintains CVE on behalf of the US National Cybersecurity Division

https://www.cve.org/
CVEs: True or false?

A project with no CVEs is more secure than a project with many CVEs.
CVEs per year

<table>
<thead>
<tr>
<th>Year</th>
<th>CVEs per year</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>6,457</td>
</tr>
<tr>
<td>2017</td>
<td>14,645</td>
</tr>
<tr>
<td>2018</td>
<td>16,512</td>
</tr>
<tr>
<td>2019</td>
<td>17,308</td>
</tr>
<tr>
<td>2020</td>
<td>18,375</td>
</tr>
<tr>
<td>2021</td>
<td>20,161</td>
</tr>
<tr>
<td>2022</td>
<td>25,059</td>
</tr>
<tr>
<td>2023</td>
<td>28,961</td>
</tr>
</tbody>
</table>

For more information, visit: https://www.cve.org/About/Metrics
So many dependencies

- Secondary and tertiary dependencies can get well into the 100s...
- Especially with web applications

https://www.drupal.org/project/composer_dependency_tree
New contributors!

From GitHub:

- 2023 had the largest number of first-time contributors
- 420 million total projects (27% growth YOY)
- 4.5 billion contributions in 2023
Evaluating projects

What does it mean to consume open source software securely?
Evaluating open source projects

1. Review basic health—Is it active?
2. Check governance—Is it defined?
3. Review maintenance & releases—Is there a cadence?
4. Explore the community—Are people engaged?
5. Bug reporting—Is there a documented process?
What’s the first thing you would look at when evaluating an open source project to use or include as a dependency?
1. Evaluating software: Basic health

- Does the project even have a maintainer anymore?
- When was the last commit?
- Look at the issue queue
  - How active is it?
  - When was the last post?
  - When was the last response to an issue?
2. Evaluating software: Governance

- Clearly defined governance?
  - Clearly stated license? (Hopefully OSI approved)
  - More than one maintainer
  - Maintainers from more than one company or organization
  - How are decisions made?

https://opensource.org/licenses
3. Evaluating software: Maintenance and release management

- Has there been substantial activity in the last year?
- Look at the release cadence
  - Is it documented?
  - Regularly occurring?
  - Prompt patch releases to address bugs and security issues?
- Does the project communicate announcements regularly?
  Does it have a blog?
- Is the latest release a “-alpha” or “-beta,” or does it indicate that it is not yet production-ready?
4. Evaluating software: Community engagement

- Contributor guide?
- Extensively used?
- Is the community working toward security best practices?
  - Automated tests
  - Up-to-date dependencies
Community

Early Bird Registration for DrupalCon Portland 2024 is open! Register by 23:59 UTC on 18 March 2024, to get $100 off your ticket.

Contribution areas

This guide is always evolving. If you'd like to help improve it, the best starting point is the Contribute to the Contributor Guide page.

The Drupal project has many areas that you can contribute to improving -- it's not

Help improve this page

Create an issue describing the problem.

https://www.drupal.org/community/contributor-guide
5. Evaluating software: Secure bug reporting

保密 bug reporting

在那里报告安全问题？

- 如果您是来报告任何类型的安全问题的，并且该问题与 a site hosted on WordPress.com 相关，则请提交 a report at the Automattic HackerOne page。如果问题不是安全问题，而是 support forums 的问题，那么请使用支持论坛。
- 如果您正在为您的自托管 WordPress.org 站点报告问题，那么请使用 WordPress.org support forums。
- 对于 WordPress 插件的安全问题，请遵循 Reporting Plugin Security Issues 的信息。
- 对于自托管的 WordPress 版本的安全问题，请在 WordPress HackerOne page 提交报告。请尽可能详细地描述问题。请直接使用 HackerOne，即使问题是 Trac trunk 或者 beta/RC 版本，因为有些站点不会使用生产环境。

在所有情况下，您都不应该在修复问题之前将细节分享给其他人。
Tools for securing open source software

Beyond basic health
Security tools for open source software

- Intel maintained CVE-bin-tool
- Open Source Security Foundation (OpenSSF):
  - OpenSSF Best Practices Badge
  - Secure Supply Chain Consumption Framework (S2C2F)
  - OpenSSF Scorecard
The CVE Binary Tool can help you find known vulnerabilities in software by using data from the National Vulnerability Database (NVD) list of Common Vulnerabilities and Exposures (CVEs) as well as known vulnerability data from Redhat, Open Source Vulnerability Database (OSV), Gitlab Advisory Database (GAD), and Curl.

1. A binary scanner—Helps you determine which packages may have been included as part of a piece of software.
2. Tools for scanning known component lists—Such as CSV files, SBOM formats, etc.

As simple as ...
pip install cve-bin-tool
cve-bin-tool <directory/file>
Open Source Security Foundation (OpenSSF)

The Open Source Security Foundation (OpenSSF) seeks to make it easy to **develop, maintain, and consume** open source software safely and securely.

This includes fostering collaboration, establishing best practices, and developing innovative solutions for the open source software we all depend on.
OpenSSF projects and tools

OpenSSF Best Practices Badge

Gramine Library OS with Intel SGX

What is Gramine?

Gramine (formerly called Graphene) is a lightweight Linux-compatible multi-process host requiring Linux binaries to run. It provides a complete OS in a virtual machine -- including guest process migration.

Gramine supports native, unmodified Linux binaries and Intel SGX enclaves on Linux platforms.

In untrusted cloud and edge deployments, there is a need to run sensitive applications on minimal infrastructure. Gramine supports this "lift and shift" of Confidential Computing with Intel SGX. Gramine can provide minimal porting effort.

Documentation

- The project MUST have a documented roadmap that describes what the project intends to do and not do for at least the next year. (URL required) [documentation_roadmap]

- The project MUST include documentation of the architecture (aka high-level design) of the software produced by the project. If the project does not produce software, select "not applicable" (N/A). (URL required) [documentation_architecture]

- The project MUST document what the user can and cannot expect in terms of security from the software produced by the project (its "security requirements"). (URL required) [documentation_security]

- The project MUST provide a "quick start" guide for new users to help them quickly do something with the software. (URL required) [documentation_quick_start]

https://www.libreoffice.org/get-help/documentation/
OpenSSF projects and tools

OpenSSF Scorecard

- What is it?
  - Quick, easy project assessment via list of automated checks for best practices

- What does it help protect me from?
  - Malicious maintainers and packages
  - Poorly maintained projects
  - Compromised build systems and/or code

- How do I use it?
  - Command line interface (CLI)
  - GitHub Action
OpenSSF projects and tools

OpenSSF Scorecard

Score in terminal ...

... or via browser

OpenSSF Scorecard Report

5.5

<table>
<thead>
<tr>
<th>Scorecard Name</th>
<th>Commit SHA</th>
<th>Score</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>python-fire</td>
<td>343eb6ce2d174511e99dec7e5a2484912c2e</td>
<td>5.5</td>
<td></td>
</tr>
</tbody>
</table>

**Dangerous-Workflow**
- CRITICAL
  - Determines if the project’s GitHub Action workflows avoid dangerous patterns.

**Branch-Protection**
- HIGH
  - Determines if the default and release branches are protected with GitHub’s branch protection settings.

**Token-Permissions**
- HIGH
  - Determines if the project’s workflows follow the principle of least privilege.

**Code-Review**
- HIGH
The S2C2F project works to further develop and improve the S2C2F guide, which outlines how to securely consume open source software (OSS) dependencies.
Putting the tools to work

Let’s evaluate some software
Evaluating open source projects

1. Review basic health—Is it active?
2. Check governance—Is it defined?
3. Review maintenance & releases—Is there a cadence?
4. Explore the community—Are people engaged?
5. Bug reporting—Is there a documented process?
6. Run OpenSSF Scorecard
OpenSSF projects and tools

Grab a random repo

You can apply some optional filters:

Language
Any Language

Topic
Any Topic

google/python-fire
Python Fire is a library for automatically generating command line interfaces (CLIs) from absolutely any Python object.

Save

Download List of Selected Repos
Open All

© 2020 DigitalBunker

https://gitrandom.digitalbunker.dev/
Basic health check: Looks promising!

Python Fire

Python Fire is a library for automatically generating command line interfaces from any Python object.

- Python Fire is a simple way to create a CLI in Python. [1]
- Python Fire is a helpful tool for developing and debugging Python code. [2]
- Python Fire helps with exploring existing code or turning other people’s code into a CLI. [3]
- Python Fire makes transitioning between Bash and Python easier. [4]
- Python Fire makes using a Python REPL easier by setting up the REPL with the modules and variables you'll need already imported and created. [5]

Installation

To install Python Fire with pip, run: `pip install fire`
To install Python Fire with conda, run: `conda install fire --c conda-forge`
To install Python Fire from source, first clone the repository and then run: `python setup.py install`

No OpenSSF Best Practices Badge?

https://github.com/google/python-fire
Issue queue

- **Cannot parse list of strings containing**
  - #481 opened 2 weeks ago by renwu-wang

- **Remove test requirement on mock**
  - #489 opened on Nov 1, 2023 by odrzy

- **Version flag alongside other commands**
  - #498 opened on Oct 11, 2023 by jerem-jeed

- **[feature request] Exclude function (kw)args from synopses, arguments and flags in help output**
  - #496 opened on Sep 28, 2023 by svenarius

- **[feature request] support multiple dialects for boolean parameters**
  - #491 opened on Aug 31, 2023 by byake

- **Warning Deprecation: Legacy "setup.py"**
  - #480 opened on Aug 17, 2023 by vini

- **Strings args do not need to be parsed.**
  - #459 opened on Jul 19, 2023 by hern

- **Fire needs to include features like in ArgParse**
  - #457 opened on Jul 3, 2023 by vhaanmomdy1

- **[Question] Even if no type hints is supplied, would python-fire accept stub files?**
  - #456 opened on May 16, 2023 by Olego-rossi

- **Add Docker Image for easier setup**
  - #455 opened on May 12, 2023 by Falcet-Ahren-1
Pull requests
OpenSSF Scorecard: Manual CLI scan—Terminal

scorecard --repo github.com/google/python-fire
## OpenSSF Scorecard: Manual CLI scan—Browser

### Scorecard Report

<table>
<thead>
<tr>
<th>Feature</th>
<th>Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>github.com/google/python-fire</td>
<td>5.5</td>
<td>Camment: 343ce6bcecd274d51e99dc7e5a24849121c2e</td>
</tr>
<tr>
<td>Generated At</td>
<td>2024-03-04</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Risk Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dangerous-Workflow</td>
<td>CRITICAL</td>
<td>Determines if the project's GitHub Action workflows avoid dangerous patterns.</td>
</tr>
<tr>
<td>Branch-Protection</td>
<td>HIGH</td>
<td>Determines if default and release branches are protected with GitHub's branch protection settings.</td>
</tr>
<tr>
<td>Token-Permissions</td>
<td>HIGH</td>
<td>Determines if the project's workflows follow the principle of least privilege.</td>
</tr>
<tr>
<td>Code-Review</td>
<td>HIGH</td>
<td>Determines if the project requires human code review before pull requests (aka merge requests) are merged.</td>
</tr>
<tr>
<td>Maintained</td>
<td>HIGH</td>
<td>Determines if the project is &quot;actively maintained&quot;.</td>
</tr>
<tr>
<td>Binary-Artifacts</td>
<td>HIGH</td>
<td>Determines if the project has generated executable (binary) artifacts in the source repository.</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>HIGH</td>
<td>Determines if the project has open, known unfixed vulnerabilities.</td>
</tr>
<tr>
<td>Fuzzing</td>
<td>MEDIUM</td>
<td>Determines if the project uses fuzzing.</td>
</tr>
<tr>
<td>Pinched-Dependencies</td>
<td>MEDIUM</td>
<td>Determines if the project has declared and pinned the dependencies of its build process.</td>
</tr>
<tr>
<td>SAST</td>
<td>MEDIUM</td>
<td>Determines if the project uses static code analysis.</td>
</tr>
<tr>
<td>Security-Policy</td>
<td>MEDIUM</td>
<td>Determines if the project has published a security policy.</td>
</tr>
<tr>
<td>CLI-Best-Practices</td>
<td>LOW</td>
<td>Determines if the project has an OpenSSF (formerly CLI) Best Practices Badge.</td>
</tr>
<tr>
<td>License</td>
<td>LOW</td>
<td>Determines if the project has defined a license.</td>
</tr>
<tr>
<td>Packaging</td>
<td>MEDIUM</td>
<td>Determines if the project is published as a package that others can easily download, install, easily update, and uninstall.</td>
</tr>
<tr>
<td>Signed-Releases</td>
<td>HIGH</td>
<td>Determines if the project cryptographically signs release artifacts.</td>
</tr>
</tbody>
</table>

[View the report](https://securityscorecards.dev/viewer/?uri=github.com/google/python-fire)
The good:
- No dangerous workflows!
- Maintained!
- Security policy!
- Even fuzzing!

The less good:
- No signed releases
- Static analysis
- Branch protection unknown
Get involved in the OpenSSF

Be your own hero!

openssf.org

The best way to influence an OSS project direction is to get involved.
Taking ownership

Developers don’t owe you anything
Scan for tools, sources, and resources

Visit the presentation’s GitHub page

- Intel and OpenSSF tools
- Guides and community resources
- Links to articles and source material
- A PDF of this presentation
Where to find me

- Twitter/X: @katherined
- Fediverse: @katherined@reality2.social
- LinkedIn: katherinedruckman
Notices and disclaimers

Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel’s Global Human Rights Principles. Intel® products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.

Intel® technologies may require enabled hardware, software, or service activation. No product or component can be absolutely secure. Your costs and results may vary.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.