



Securing Eclipse Foundation's Projects Software Supply Chain

Bitkom Forum Open Source

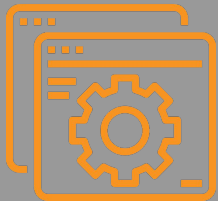
September, 27th 2023
Mikaël Barbero

Open Source Software Security - A Realization

80-90%



**Open source
makes up 80-90%
of applications**



**Today, you can't
develop software
without doing open
source!**

— Mercedes Benz

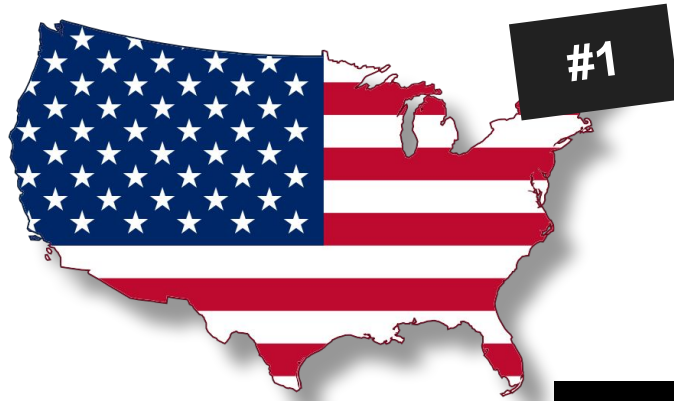
Source: Forrester



Crime Pays

COPYRIGHT (C) 2023, ECLIPSE FOUNDATION, INC. | THIS WORK IS LICENSED UNDER A CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE (CC BY 4.0)

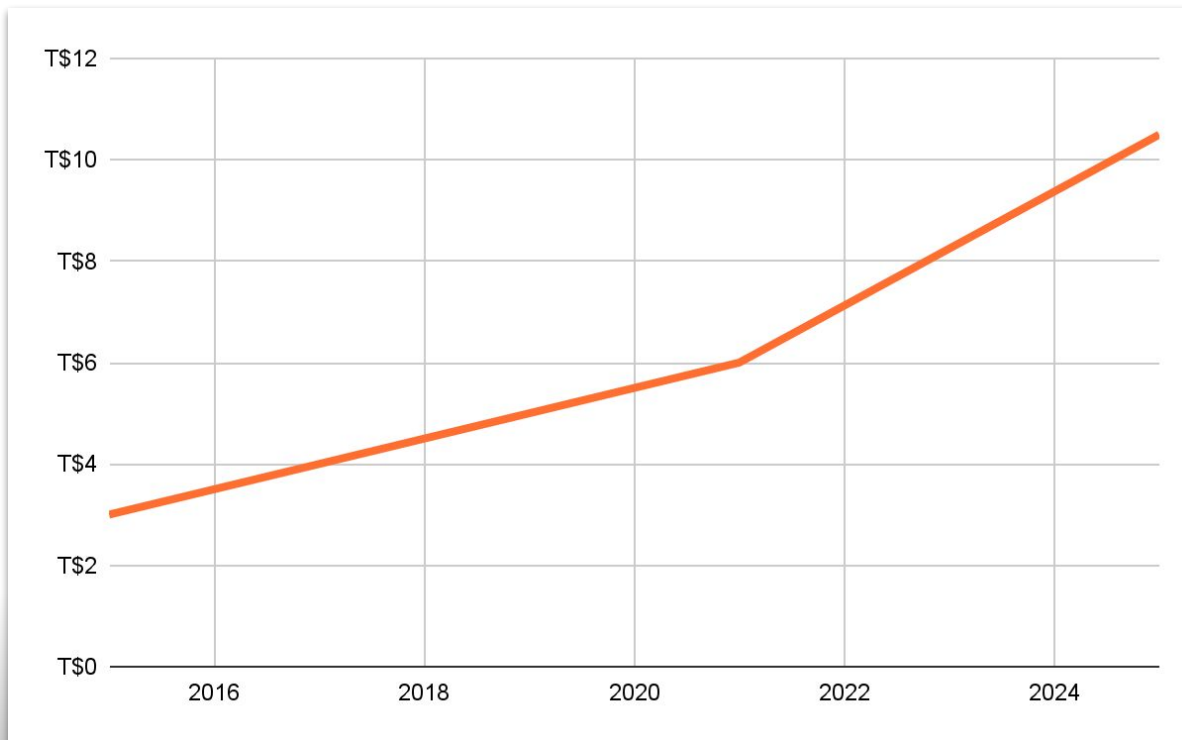
Cybercrime: World's 3rd Largest Economy



<https://10guards.com/en/articles/cybercrime-as-empire-would-be-the-worlds-third-largest-economy/>

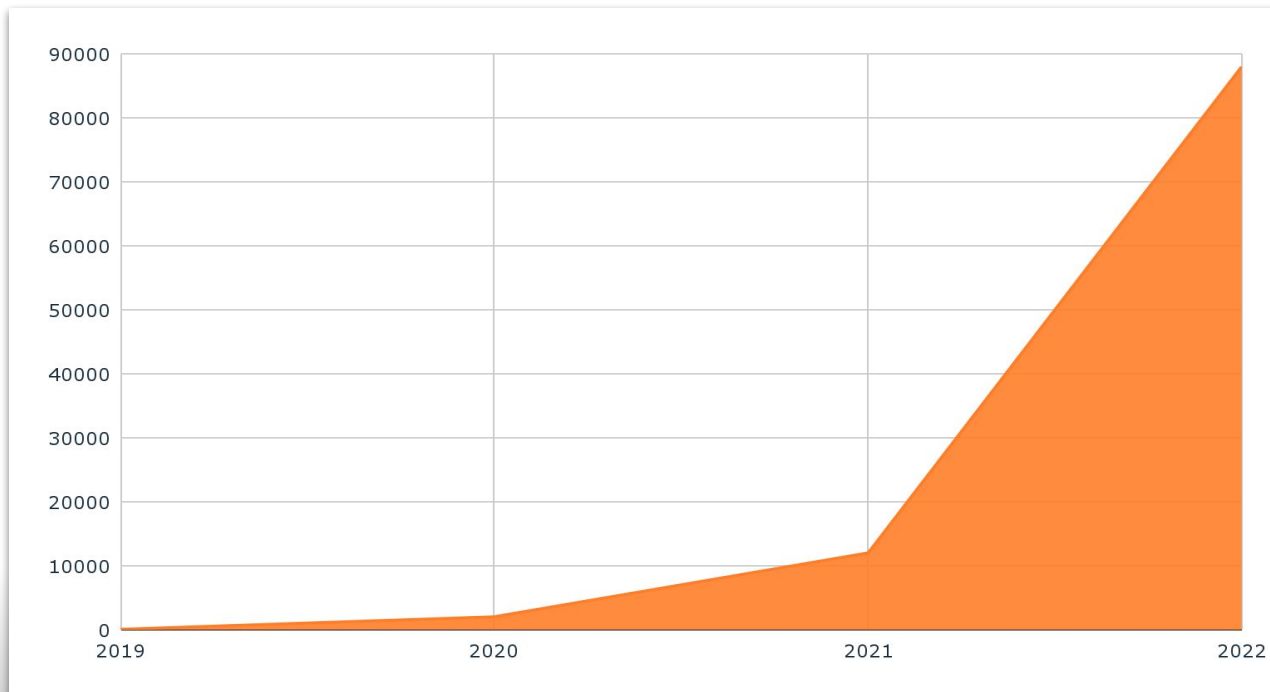
COPYRIGHT (C) 2023, ECLIPSE FOUNDATION. | THIS WORK IS LICENSED UNDER A CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE (CC BY 4.0)

Costs to World Economy reaching \$10.5 Trillion by 2025



<https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

Software Supply Chain Attacks increase 742% in 3 years

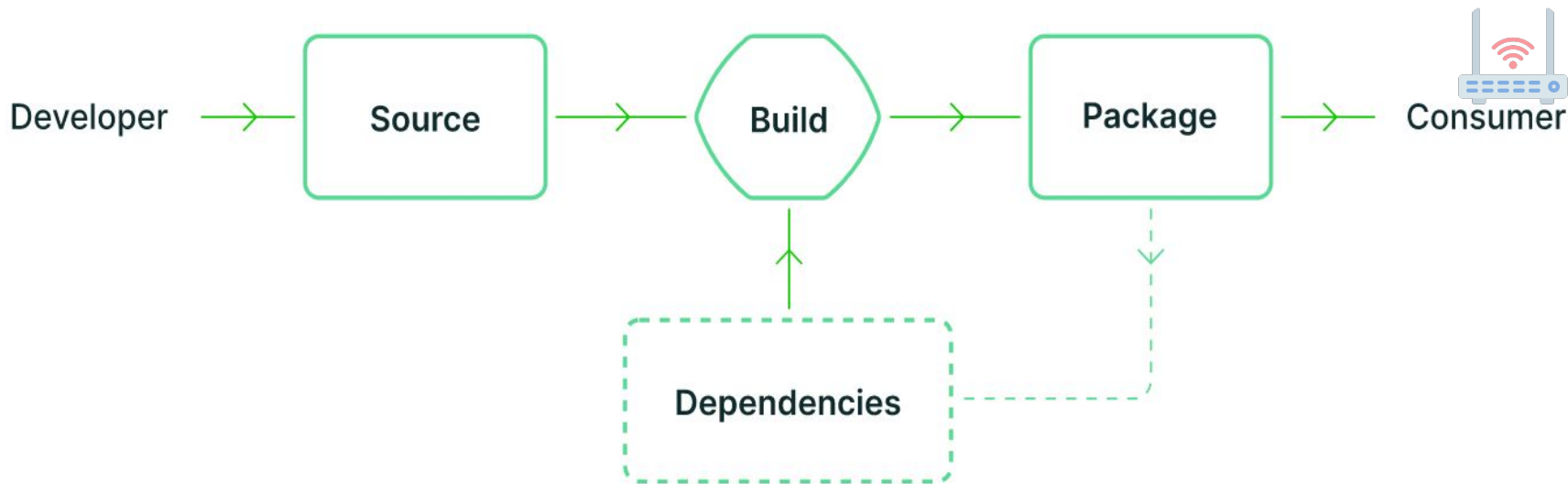


<https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-demand-security>



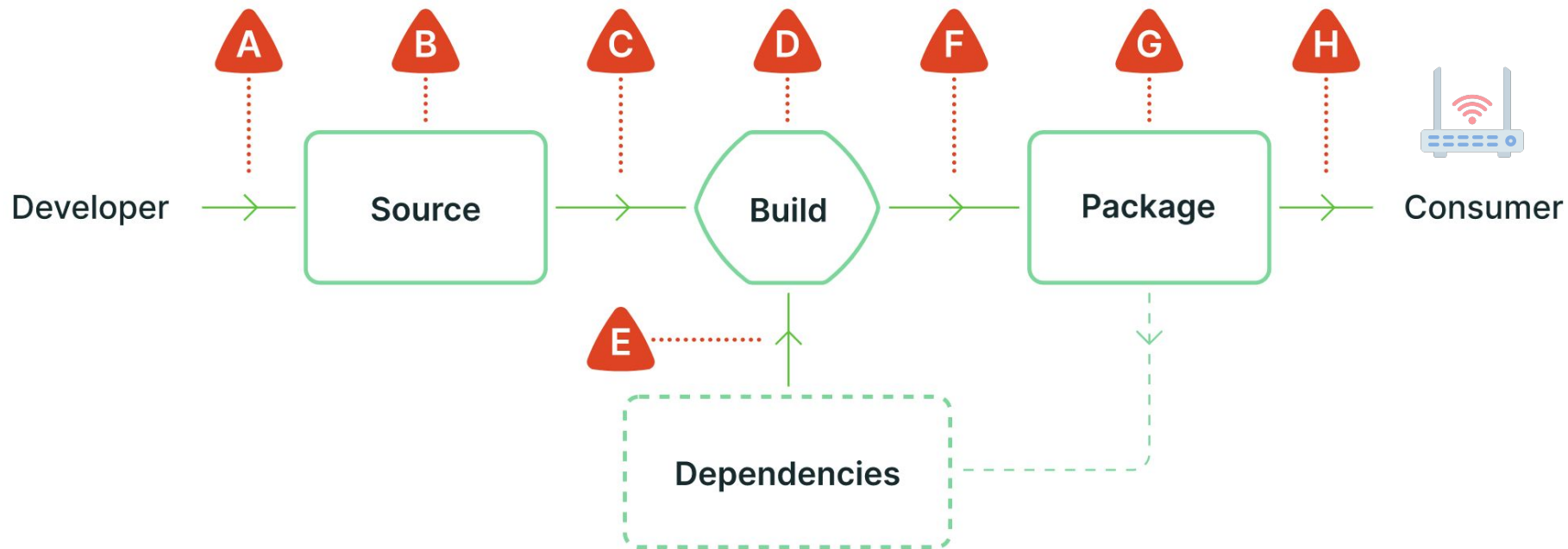
Global Supply Chain

What is a Software Supply Chain?



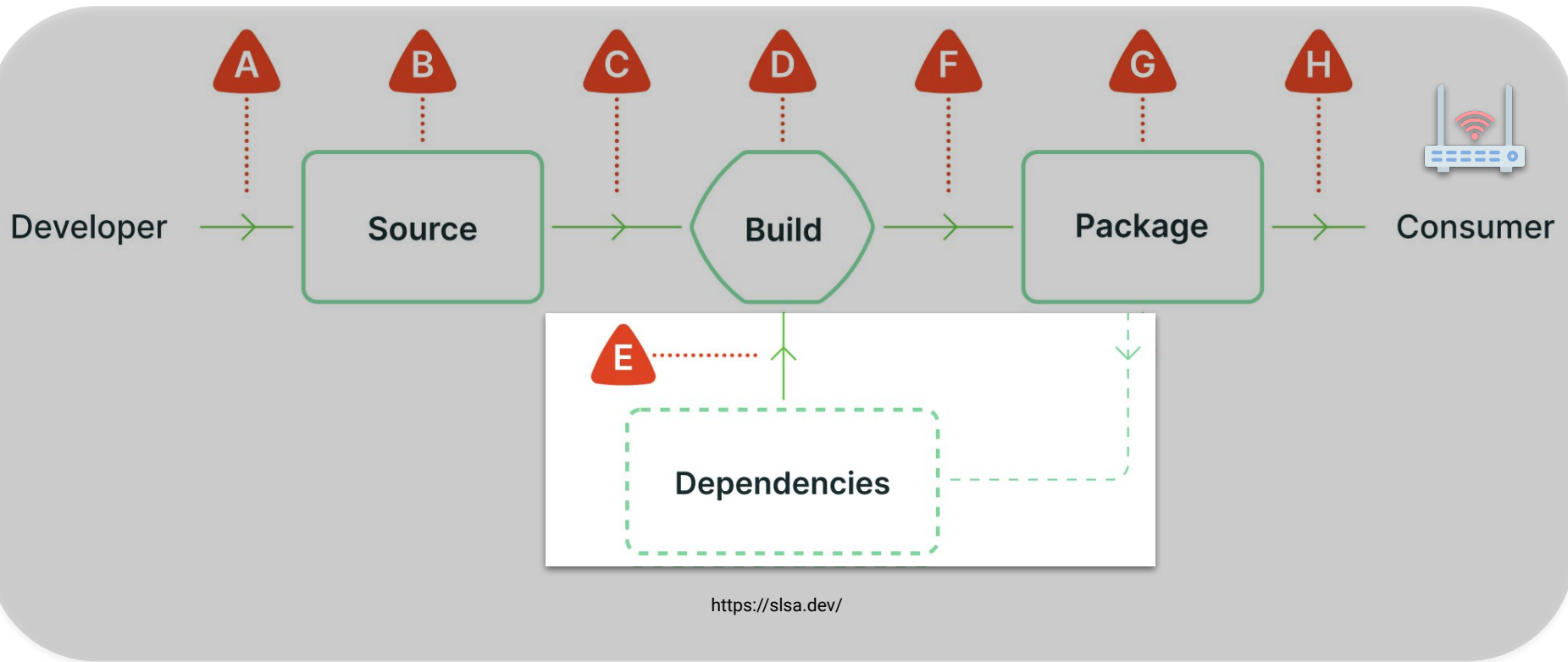
<https://slsa.dev/>

Where are the Threats?

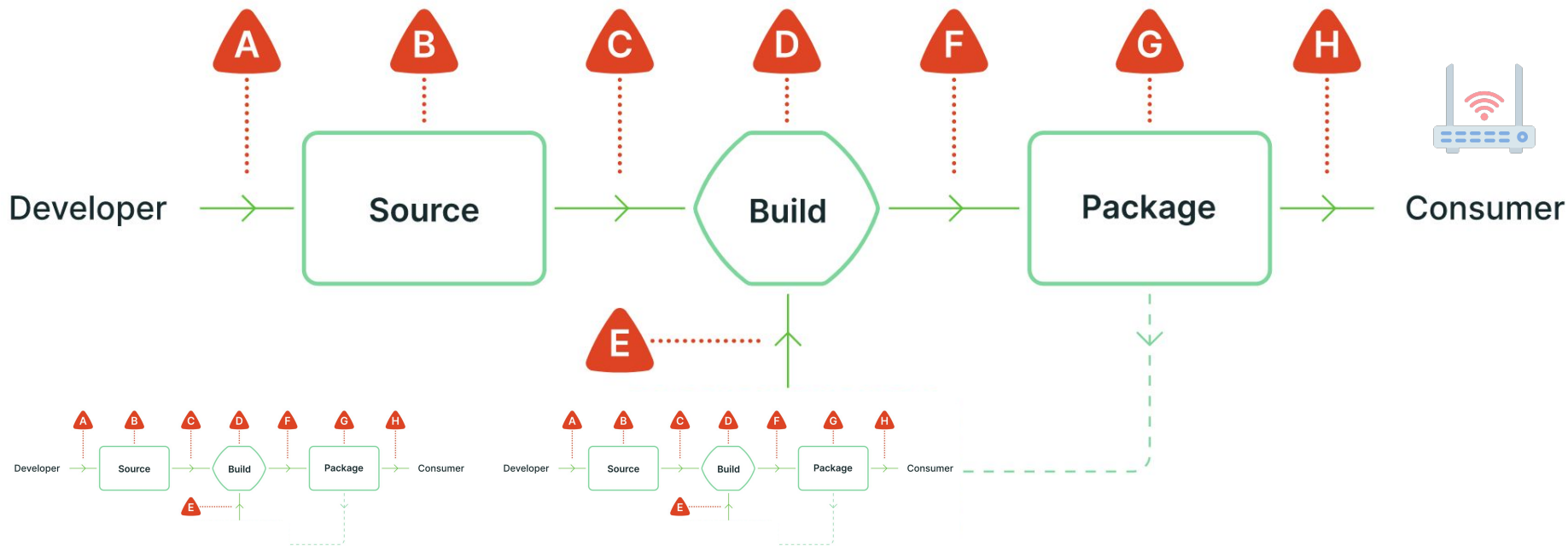


<https://slsa.dev/>

Where are the Threats?

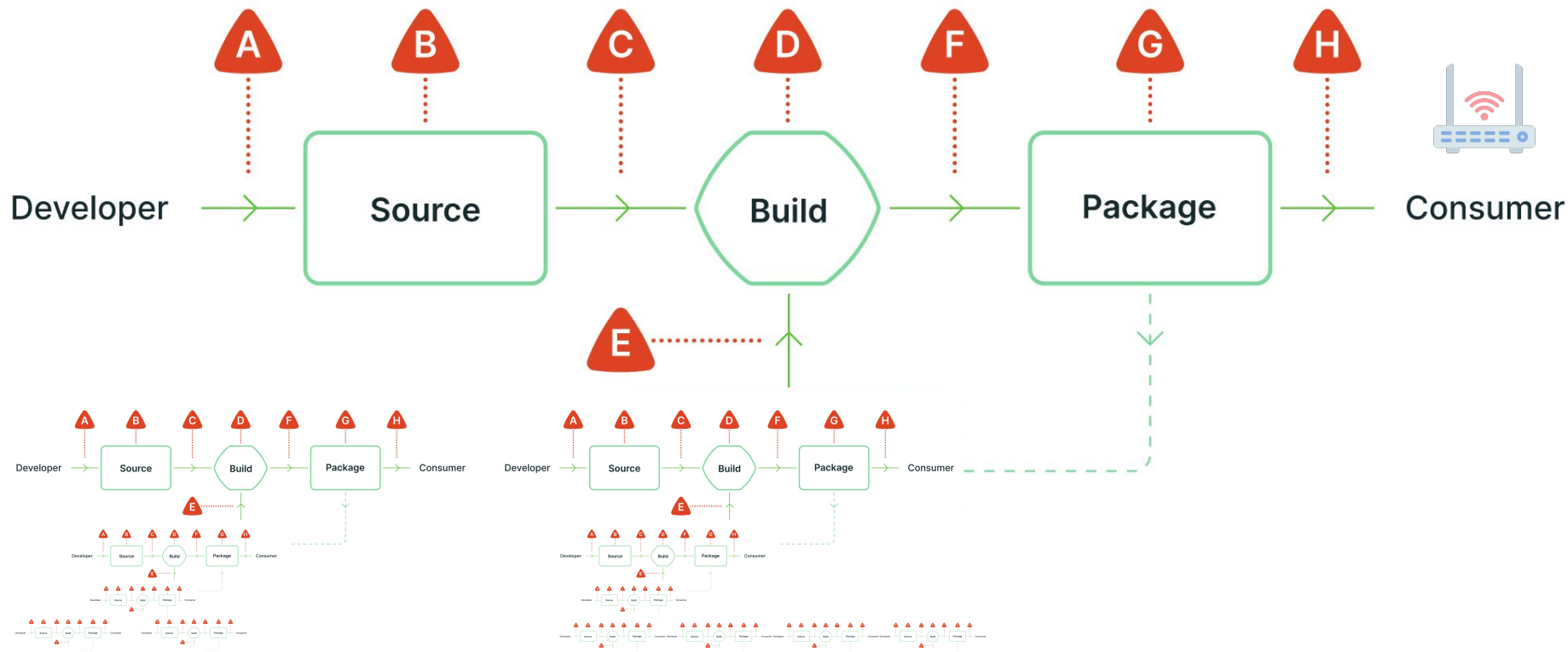


Where are the Threats?



<https://slsa.dev/>

Where are the Threats?

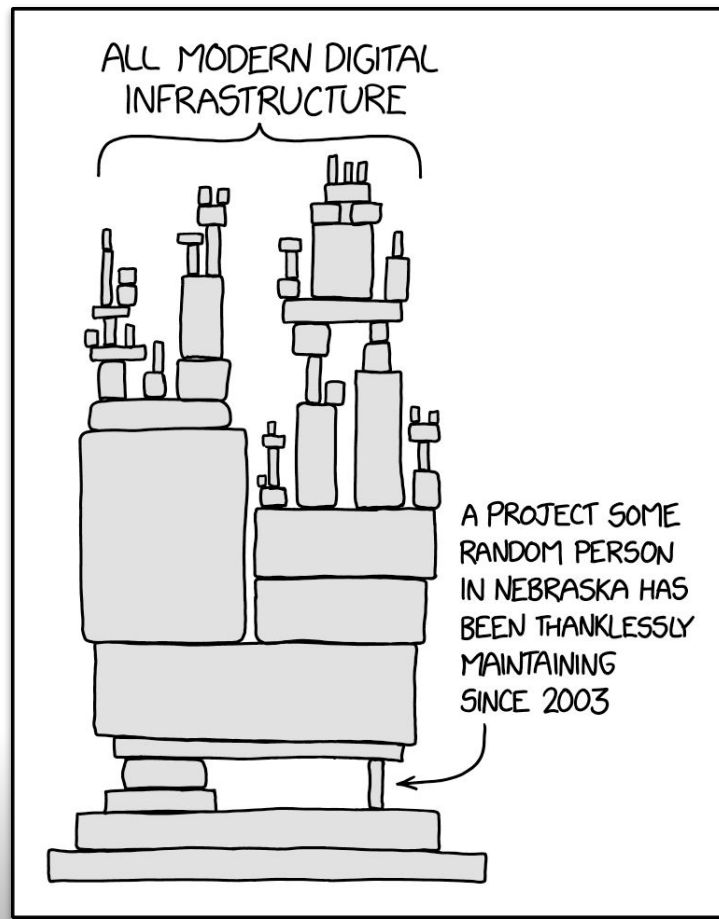


<https://slsa.dev/>

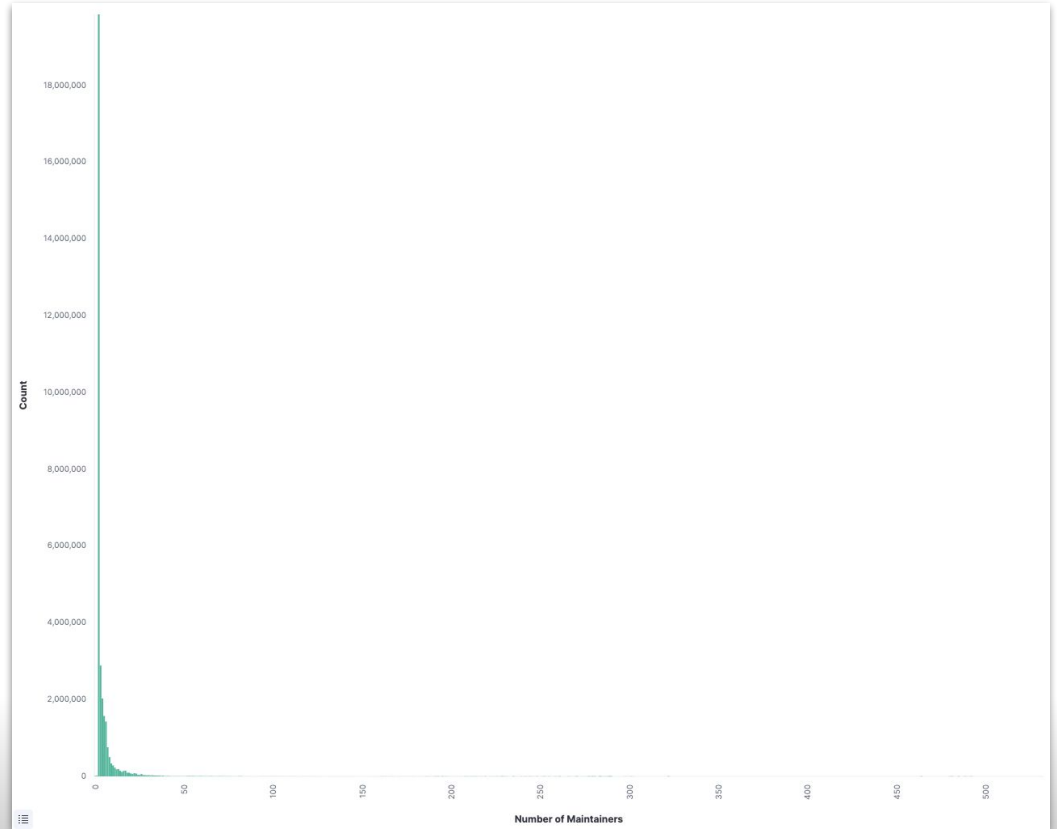


Who Maintains The Supply Chain?

Dependencies

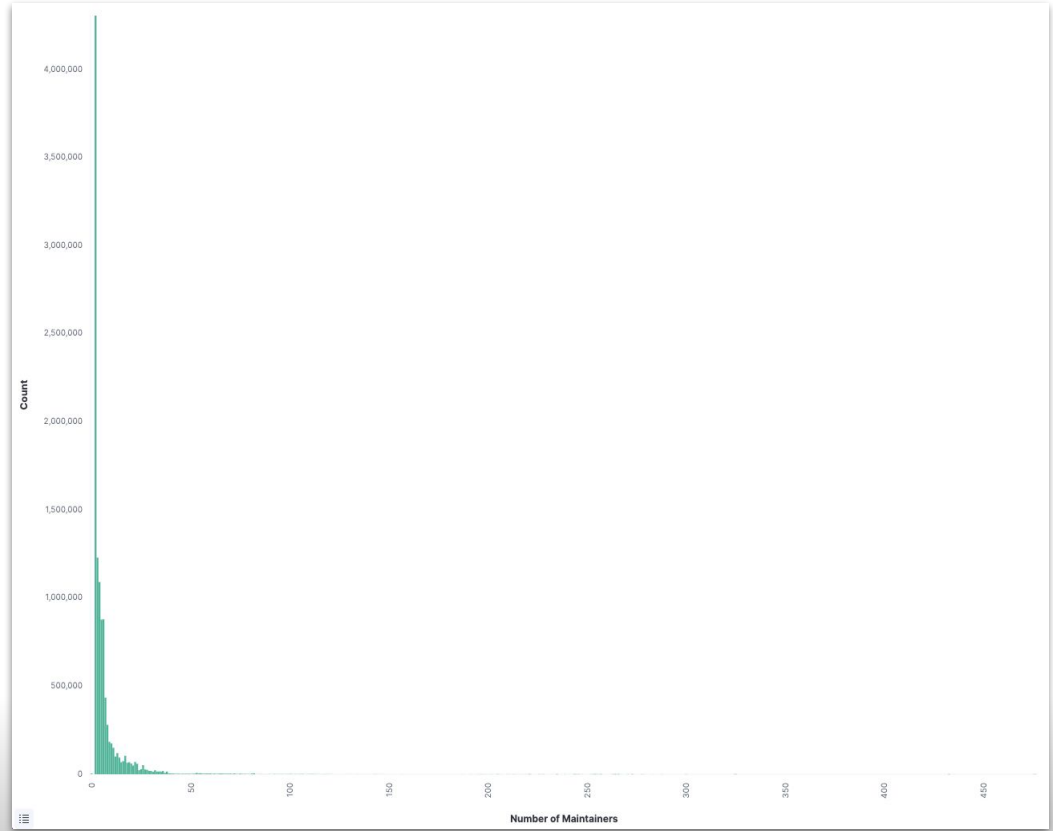


npm Dependency Maintainers



Source: <https://anchore.com/blog/open-source-is-bigger-than-you-imagine/>

npm Dependency Maintainers (top 5%)



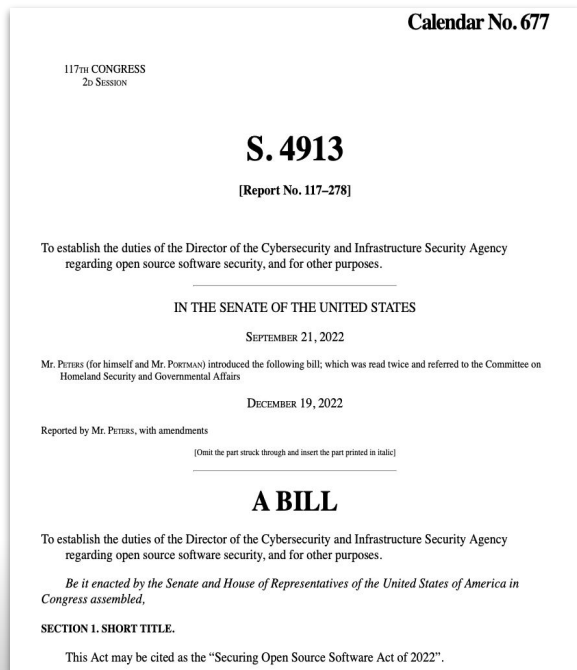
Source: <https://anchore.com/blog/open-source-is-bigger-than-you-imagine/>

Open Source Software Security - A Realization



The next
log4shell is
coming our way!

Governments have started to notice



Eclipse Foundation Challenge

**Know how to react
to next Log4Shell?**

Massive reputational risk

**Supply Chain Security
is technical debt**

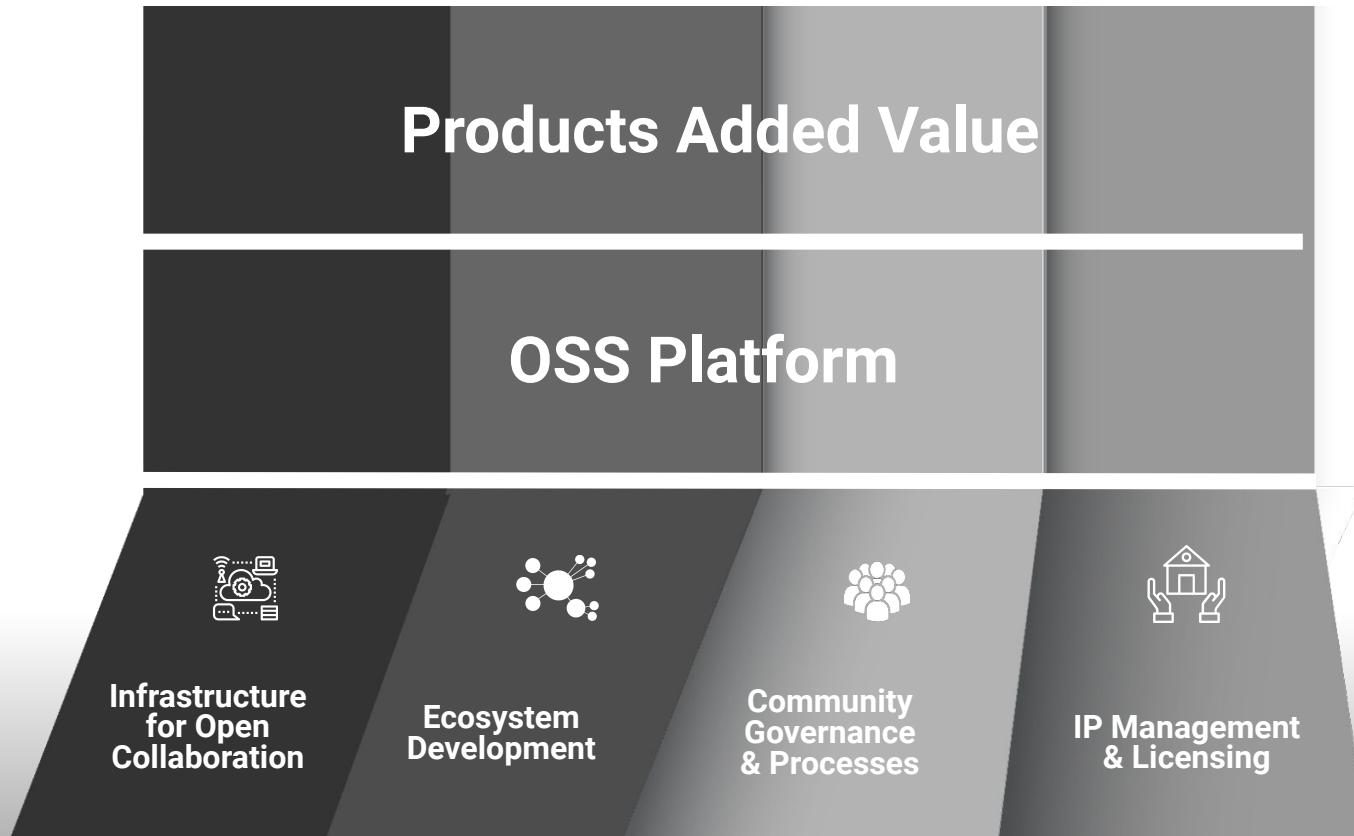
Unlikely that developers will be able
to address it on their own

Vision

**To be the leading open
source foundation
globally in implementing
supply chain security
best practices**



Eclipse Foundation



Products Added Value

OSS Platform



**Infrastructure
for Open
Collaboration**



**Ecosystem
Development**



**Community
Governance
& Processes**

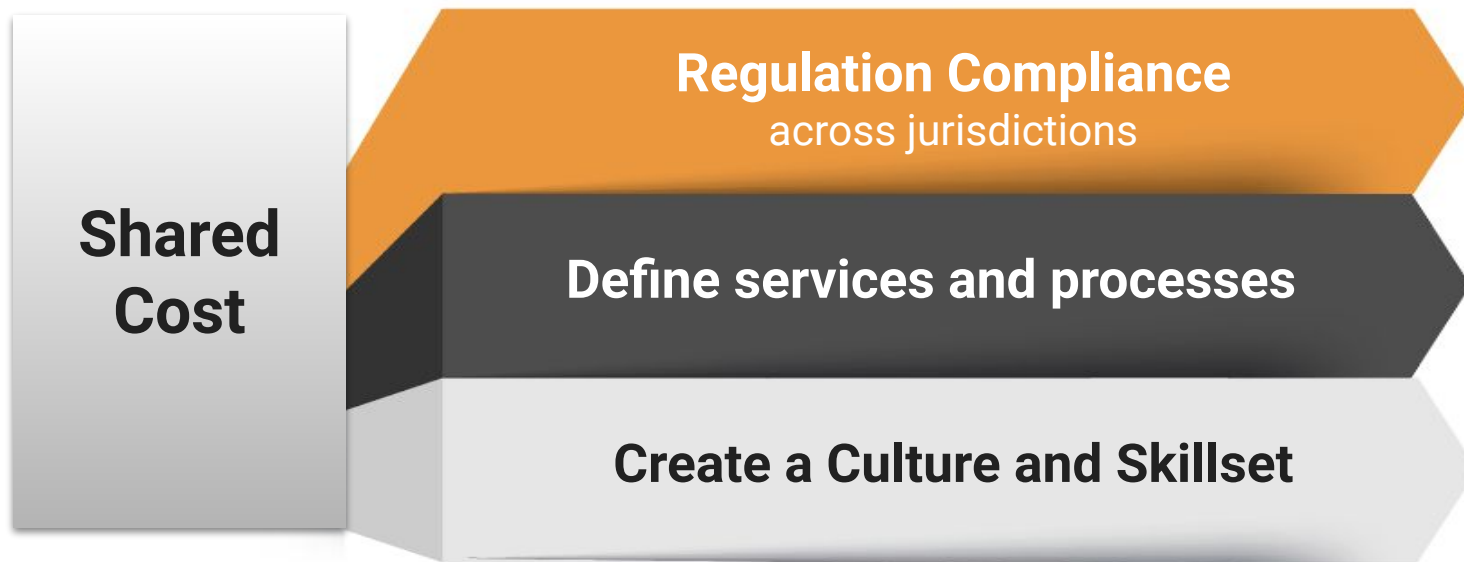


**IP Management
& Licensing**

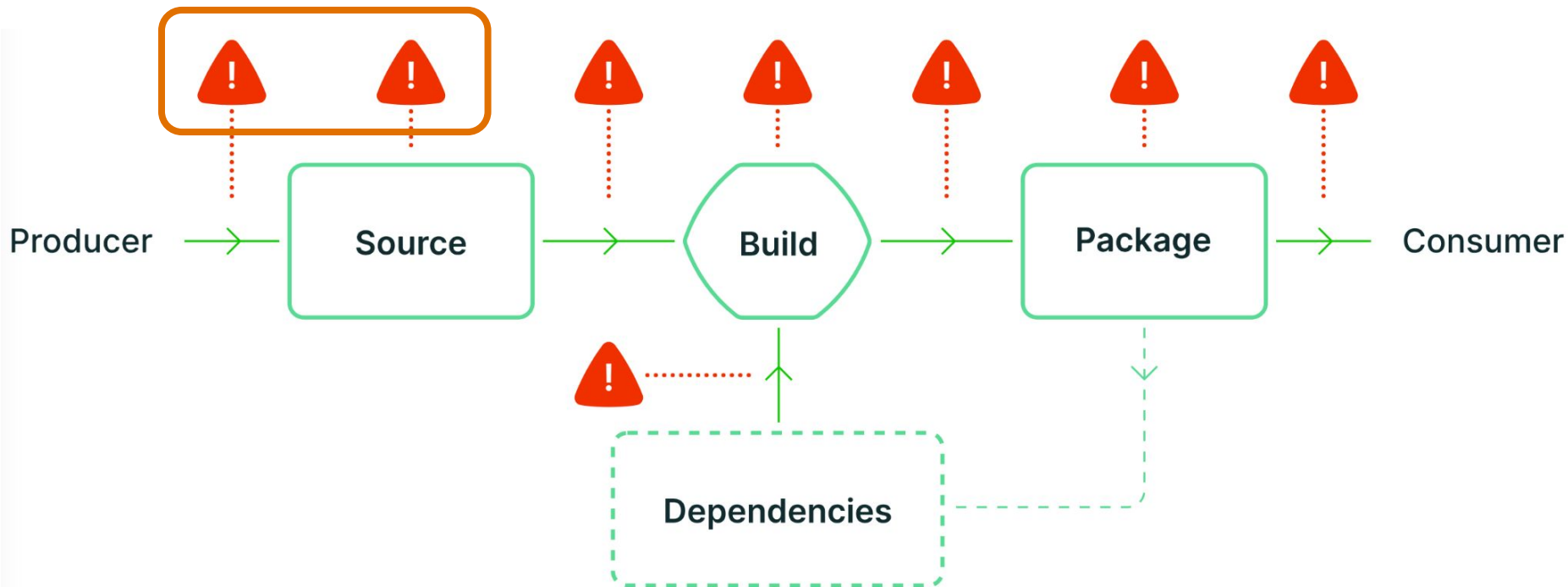


**Supply Chain
Security**

Security - Community Effort



Software Supply Chain & Threats



Security Audits



Security Assessment of OSTIF's Eclipse Application with Threat Model



Page 3 of 25
Privileged and Confidential
Report

TRAIL
of
BITS

Eclipse JKube

Security Assessment

15 May, 2023

Prepared for:

Marc Nuri San Felix
The Eclipse Foundation

Organized by the Open Source Technology Improvement Fund, Inc.

Prepared by: Artur Cygan and Emilio López

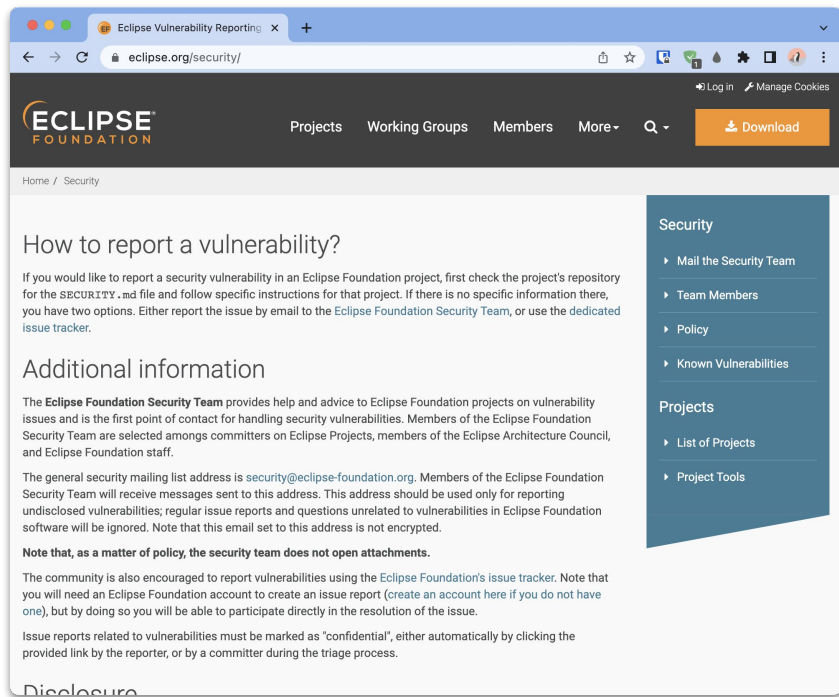
TRAIL
of
BITS

OSTIF.org

Open Source Technology
Improvement Fund
Securing Open Source for the World

TRAIL
of
BITS

Vulnerability reports management



The screenshot shows the Eclipse Vulnerability Reporting page. The header includes the Eclipse Foundation logo and navigation links: Projects, Working Groups, Members, More, and a search icon. A 'Download' button is also present. The main content area is titled 'How to report a vulnerability?' and provides instructions on how to report a security vulnerability in an Eclipse Foundation project. It mentions that if there is no specific information, users have two options: report the issue by email to the Eclipse Foundation Security Team or use the dedicated issue tracker. Below this, there is a section titled 'Additional information' which states that the Eclipse Foundation Security Team provides help and advice on vulnerability issues and is the first point of contact for handling security vulnerabilities. It also mentions that the general security mailing list address is security@eclipse-foundation.org. A note states that the security team does not open attachments. The page also encourages reporting vulnerabilities using the Eclipse Foundation's issue tracker. A sidebar on the right contains links for Security (Mail the Security Team, Team Members, Policy, Known Vulnerabilities) and Projects (List of Projects, Project Tools).

Eclipse Vulnerability Reporting

eclipse.org/security/

Log in Manage Cookies

ECLIPSE FOUNDATION

Projects Working Groups Members More Search Download

Home / Security

How to report a vulnerability?

If you would like to report a security vulnerability in an Eclipse Foundation project, first check the project's repository for the SECURITY.md file and follow specific instructions for that project. If there is no specific information there, you have two options. Either report the issue by email to the Eclipse Foundation Security Team, or use the dedicated issue tracker.

Additional information

The Eclipse Foundation Security Team provides help and advice to Eclipse Foundation projects on vulnerability issues and is the first point of contact for handling security vulnerabilities. Members of the Eclipse Foundation Security Team are selected among committers on Eclipse Projects, members of the Eclipse Architecture Council, and Eclipse Foundation staff.

The general security mailing list address is security@eclipse-foundation.org. Members of the Eclipse Foundation Security Team will receive messages sent to this address. This address should be used only for reporting undisclosed vulnerabilities; regular issue reports and questions unrelated to vulnerabilities in Eclipse Foundation software will be ignored. Note that this email set to this address is not encrypted.

Note that, as a matter of policy, the security team does not open attachments.

The community is also encouraged to report vulnerabilities using the Eclipse Foundation's issue tracker. Note that you will need an Eclipse Foundation account to create an issue report (create an account here if you do not have one), but by doing so you will be able to participate directly in the resolution of the issue.

Issue reports related to vulnerabilities must be marked as "confidential", either automatically by clicking the provided link by the reporter, or by a committer during the triage process.

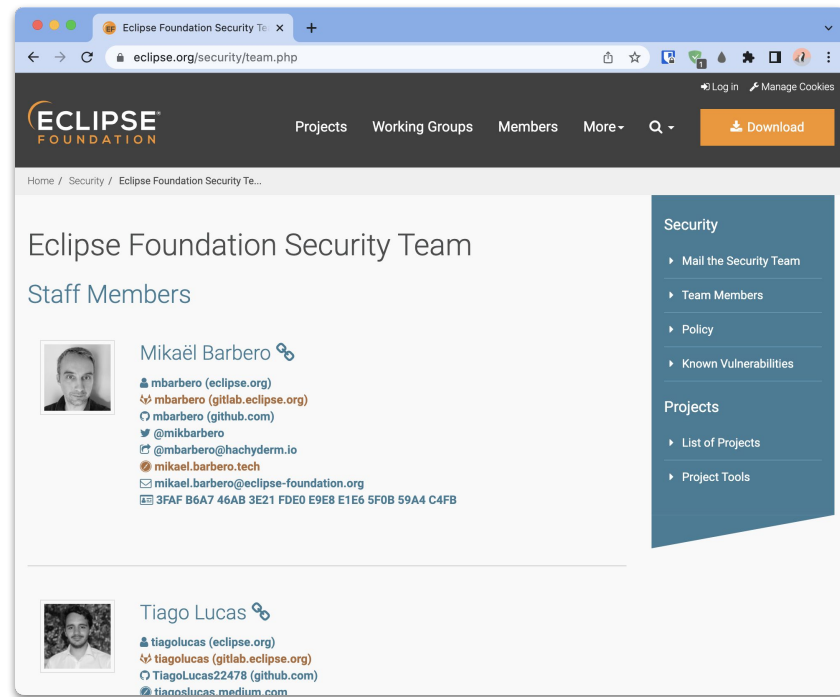
Disclosure

Security

- Mail the Security Team
- Team Members
- Policy
- Known Vulnerabilities

Projects

- List of Projects
- Project Tools



The screenshot shows the Eclipse Foundation Security Team page. The header is similar to the previous page, with the Eclipse Foundation logo and navigation links. The main content area is titled 'Eclipse Foundation Security Team' and 'Staff Members'. It features profiles for two team members: Mikael Barbero and Tiago Lucas. Mikael Barbero's profile includes his name, a photo, and links to his Eclipse.org, GitHub, and Medium profiles. Tiago Lucas's profile also includes his name, a photo, and links to his Eclipse.org, GitHub, and Medium profiles. A sidebar on the right contains links for Security (Mail the Security Team, Team Members, Policy, Known Vulnerabilities) and Projects (List of Projects, Project Tools).

Eclipse Foundation Security Team

eclipse.org/security/team.php

Log in Manage Cookies

ECLIPSE FOUNDATION

Projects Working Groups Members More Search Download

Home / Security / Eclipse Foundation Security Team

Eclipse Foundation Security Team

Staff Members

Mikael Barbero

[mbarbero \(eclipse.org\)](#)
[mbarbero \(gitlab.eclipse.org\)](#)
[mbarbero \(github.com\)](#)
[@mikbarbero](#)
[@mbarbero@hachyderm.io](#)
[mikael.barbero.tech](#)
[mikael.barbero@eclipse-foundation.org](#)
3F4F B6A7 46AB 3E21 FDE0 E9E8 E1E6 5F0B 59A4 C4F8

Tiago Lucas

[tiagolucas \(eclipse.org\)](#)
[tiagolucas \(gitlab.eclipse.org\)](#)
[TiagoLucas22478 \(github.com\)](#)
[tiagoslucas.medium.com](#)

Security

- Mail the Security Team
- Team Members
- Policy
- Known Vulnerabilities

Projects

- List of Projects
- Project Tools

Security Policy

How To Report a Vulnerability

If you think you have found a vulnerability in you can report it using one of the following ways:

- Contact the [Eclipse Foundation Security Team](#)
- Create a [confidential issue](#)

You can find more information about reporting and disclosure at the [Eclipse Foundation Security page](#).

Supported Versions

Supported versions are:

- <version 1>
- ...

Security Policy

This project follows [Eclipse Foundation Vulnerability Reporting Policy](#).

<https://gitlab.eclipse.org/security/best-practices/-/blob/main/templates/SECURITY.md>

GitHub Private Advisories

Report a vulnerability

This submission will only be viewable to repository maintainers. You will be credited if the advisory is accepted.

Advisory Details

Title *

Description *

Write

Preview

Summary

Short summary of the problem. Make the impact and severity as clear as possible. For example: An unsafe deserialization vulnerability allows any unauthenticated user to execute arbitrary code on the server.

Details

Give all details on the vulnerability. Pointing to the incriminated source code is very helpful for the maintainer.

PoC

Complete instructions, including specific configuration details, to reproduce the vulnerability.

Impact

What kind of vulnerability is it? Who is impacted?

Attach files by dragging & dropping, selecting or pasting them.

Security Advisories

View known security vulnerabilities and report new vulnerabilities privately to maintainers.

Report a vulnerability

2 Triage

1 Draft

0 Published

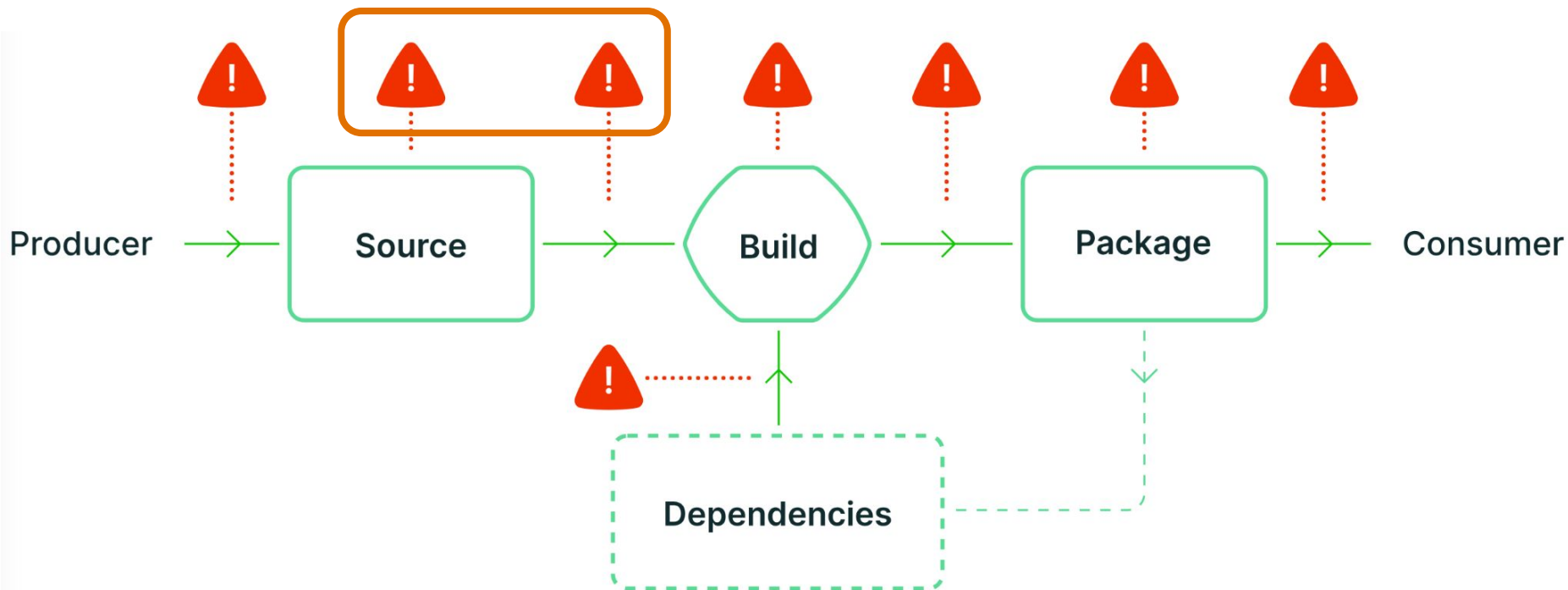
0 Closed

rj4u4

GHSA-6cpw-v4px-7xx6 opened on Nov 1, 2022 by security-researcher

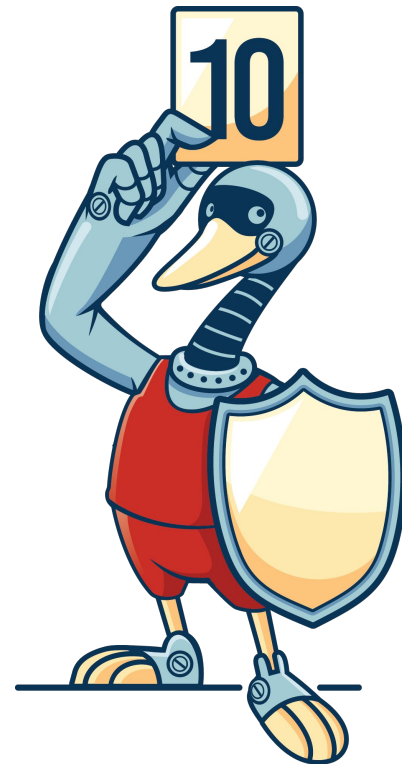
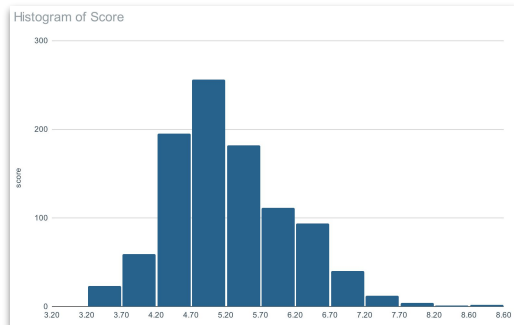
Triage

Software Supply Chain & Threats



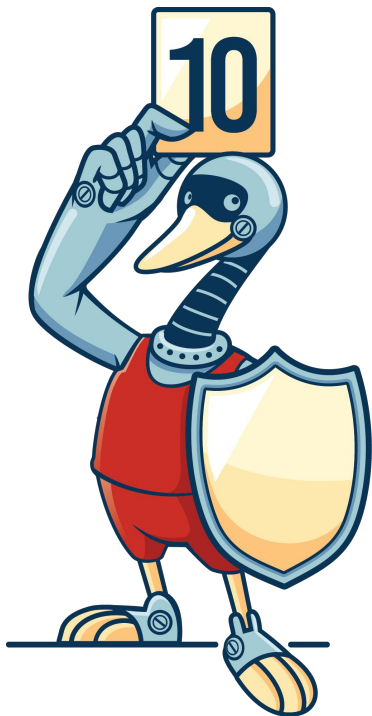
OpenSSF Scorecard

- Automated tool that assesses a number of important heuristics ("checks") associated with software security
- Assigns each check a score of 0-10
- We consider it as a trends indicator
 - Reaching a score of 10 is not necessarily a goal, nor is it desirable.

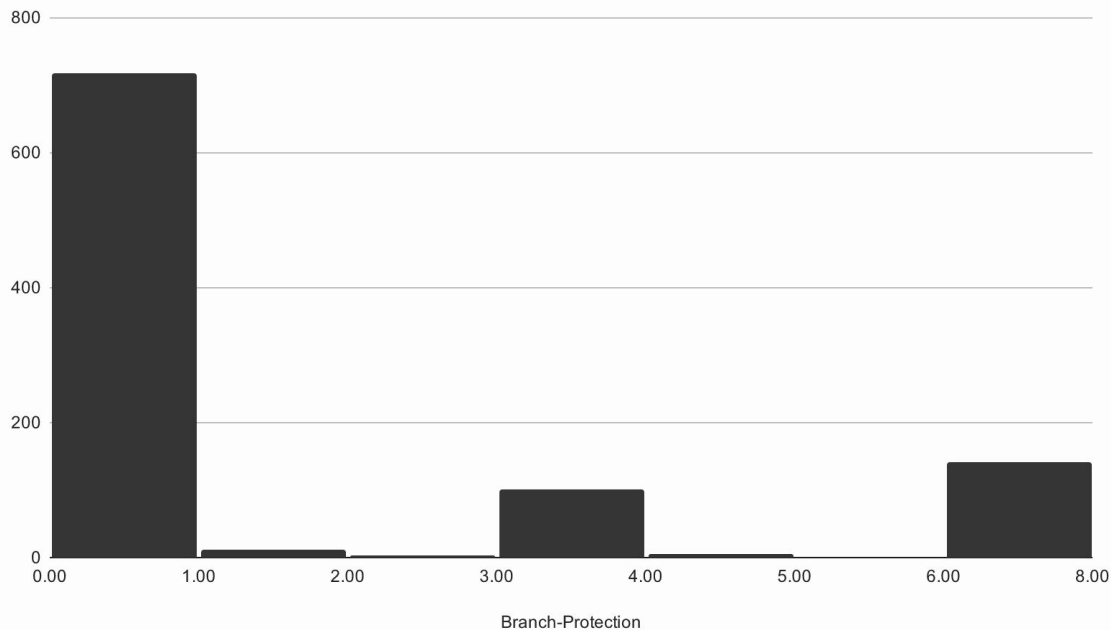


<https://github.com/ossf/scorecard>

How it started...



Histogram of Branch-Protection



<https://mikael.barbero.tech/blog/post/eclipsefdn-scorecard-aug2022/>

Taming the Octocat, at our scale!

150+

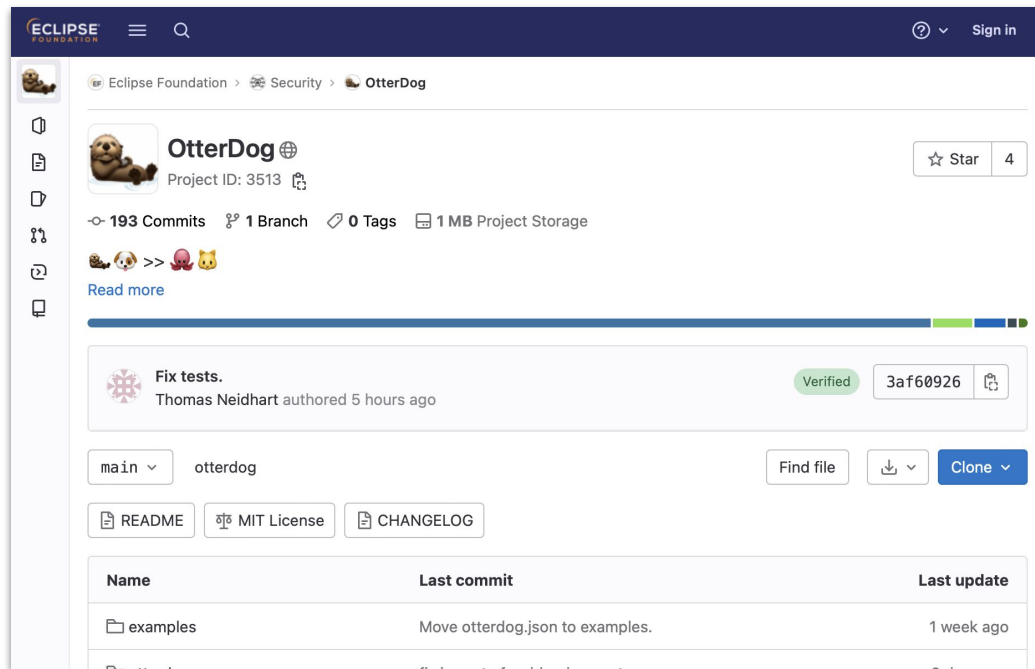
GitHub Organizations...
and counting!

1000+

GitHub Repositories...
and counting!



...how it's going!




The screenshot shows the Eclipse Foundation GitLab interface for the OtterDog project. The header includes the Eclipse Foundation logo, navigation icons, and a search bar. The breadcrumb trail is "Eclipse Foundation > Security > OtterDog". The project name "OtterDog" is displayed with a globe icon and "Project ID: 3513". A star button shows 4 stars. The project statistics are: 193 Commits, 1 Branch, 0 Tags, and 1 MB Project Storage. A commit message "Fix tests." by Thomas Neidhart is shown, verified, with commit ID 3af60926. Below the commit, there are buttons for "main", "otterdog", "Find file", "Clone", "README", "MIT License", and "CHANGELOG". A table lists the commit details:

Name	Last commit	Last update
examples	Move otterdog.json to examples.	1 week ago



<https://gitlab.eclipse.org/eclipsefdn/security/otterdog>

In one sentence!

 Otterdog configuration @ eclipse-cbi

Overview Current configuration Playground

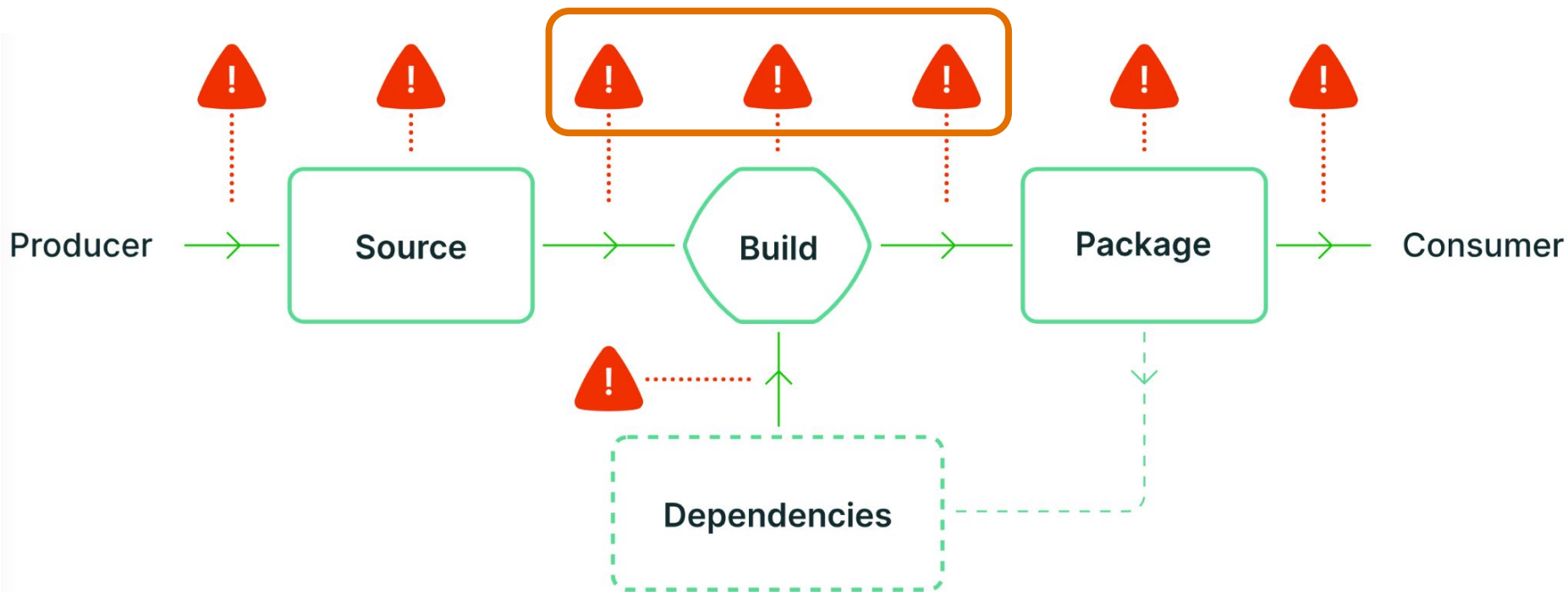
Current configuration

Organization Settings Organization Webhooks Organization Secrets **Repositories**

Repository	Branch Protection Rules	Secrets	Webhooks	Secret Scanning
.eclipsefdn	✓	✗	✗	✓
.github	✓	✗	✗	✓
ansible-playbooks	✓	✗	✗	✓
best-practices	✓	✗	✗	✓
buildkitd-okd	✓	✗	✗	✓
ci-admin	✓	✗	✗	✓

Command line tool to administer GitHub resources, such as organization and repository settings, as code

Software Supply Chain & Threats



SLSA

- Set of incrementally adoptable guidelines for supply chain security



<https://slsa.dev>

Implementer	Requirement	Degree	L1	L2	L3
Producer	Choose an appropriate build platform		✓	✓	✓
	Follow a consistent build process		✓	✓	✓
	Distribute provenance		✓	✓	✓
Build platform	Provenance generation	Exists	✓	✓	✓
		Authentic		✓	✓
		Unforgeable			✓
	Isolation strength	Hosted		✓	✓
		Isolated			✓

SLSA



<https://slsa.dev>

```
$ slsa-verifier verify-artifact my-binary \  
  --provenance-path my-binary.intoto.jsonl \  
  --source-uri github.com/my-org/my-project \  
  --source-tag v1.5.3
```

Verified signature against tlog entry index 3189970 at URL:

<https://rekor.sigstore.dev/api/v1/log/entries/206071d5ca7a2346e4db4dcb19a648c7f13b4957e655f4382b735894059bd199>

Verified build using builder

https://github.com/slsa-framework/slsa-github-generator/.github/workflows/builder_go_slsa3.yml@refs/tags/v1.2.0 at commit 5bb13ef508b2b8ded49f9264d7712f1316830d10

PASSED: Verified SLSA provenance

SLSA



<https://slsa.dev>

github.com/slsa-framework/slsa-github-generator

Code Issues 203 Pull requests 11 Actions Projects Security Insights

slsa-github-generator Public Watch 13 Fork 69 Star 220

main 7 branches 23 tags

Go to file Add file Code

renovate-bot chore(deps): update npm dev (#2302) ✓ df0719d yesterday 823 commits

.github	chore(deps): update npm dev (#2302)	yesterday
actions	chore(deps): update npm dev (#2302)	yesterday
github	fix(deps): update module github.com/google/go-github/v52 ...	yesterday
images	doc tweaks (#199)	last year
internal	feat: Add BYOB Bazel Builder (#2267)	yesterday
signing	chore: Add license headers (#2157)	last month
slsa	fix(deps): update module github.com/google/go-github/v52 ...	yesterday
version	golanglintci settings (#393)	last year
.gignore	fix: markdownlint looking in .git (#2160)	last month
.golanci.yml	chore: golanci-lint update (#2248)	2 weeks ago
.markdownlint.yml	chore: Add license headers (#2157)	last month
.markdownlintignore	ci: Add markdownlint linter (#1675)	2 months ago
.yamllint.yml	chore: Add license headers (#2157)	last month
BYOB.md	docs: Hardening BYOB (#2241)	last week
CHANGELOG.md	docs: Update CHANGELOG for v1.7.0 (#2196)	2 weeks ago
CODEOWNERS	docs: Add security policy. (#1262)	4 months ago
CODE_OF_CONDUCT.md	docs: Use CoC in governance repo (#1301)	7 months ago

About

Language-agnostic SLSA provenance generation for Github Actions

security security-hardening security-tools slsa slsaprovenance

Readme Apache-2.0 license Code of conduct Security policy Activity 220 stars 13 watching 69 forks Report repository

Releases 23

v1.7.0 Latest 2 weeks ago + 22 releases

Used by 17

SLSA

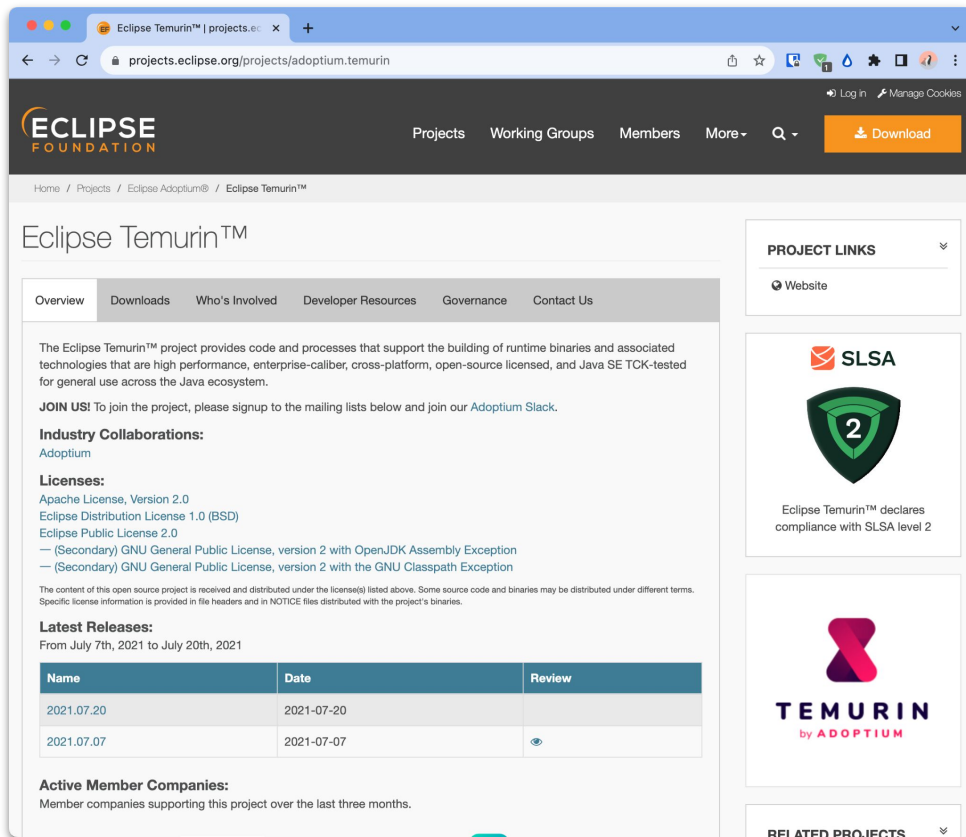


<https://slsa.dev>

The screenshot shows the GitHub repository page for 'jenkinsci/slsa-plugin'. The repository is public and has 1 branch and 0 tags. The file list includes .github, .mvn, docs/images, src, .gitignore, Jenkinsfile, LICENSE, README.md, and pom.xml. The README.md file is selected, showing the title 'SLSA Jenkins Plugin' and a description: 'The SLSA Jenkins plugin generates SLSA provenance attestations for build artifacts.' The job configuration is for a Freestyle project. The repository has 25 commits, 1 star, and 2 watchers.

File	Description	Commit Date
.github	Fix branch for release-drafter.	2 months ago
.mvn	Add .github and .mvn directories from plugin archetype.	2 months ago
docs/images	Update README.md.	2 months ago
src	Cleanup imports.	2 months ago
.gitignore	Initial commit.	2 months ago
Jenkinsfile	Initial commit.	2 months ago
LICENSE	Initial commit	2 months ago
README.md	Add support for pipeline projects, cleanup dependencies, ad...	2 months ago
pom.xml	Add support for pipeline projects, cleanup dependencies, ad...	2 months ago

SLSA



The screenshot shows the Eclipse Temurin project page. The header includes the Eclipse Foundation logo and navigation links: Projects, Working Groups, Members, More, and a Download button. The main content area is titled 'Eclipse Temurin™' and has tabs for Overview, Downloads, Who's Involved, Developer Resources, Governance, and Contact Us. The Overview tab is active, showing a description of the project, a 'JOIN US!' call to action, 'Industry Collaborations' (Adoptium), 'Licenses' (Apache License, Version 2.0; Eclipse Distribution License 1.0 (BSD); Eclipse Public License 2.0), and 'Latest Releases' (From July 7th, 2021 to July 20th, 2021). A table lists two releases: 2021.07.20 and 2021.07.07. The 'Active Member Companies' section mentions member companies supporting the project. On the right, there are 'PROJECT LINKS' (Website), an 'SLSA' badge indicating compliance with SLSA level 2, and the 'TEMURIN by ADOPTIUM' logo.

Overview Downloads Who's Involved Developer Resources Governance Contact Us

The Eclipse Temurin™ project provides code and processes that support the building of runtime binaries and associated technologies that are high performance, enterprise-caliber, cross-platform, open-source licensed, and Java SE TCK-tested for general use across the Java ecosystem.

JOIN US! To join the project, please signup to the mailing lists below and join our [Adoptium Slack](#).

Industry Collaborations:
[Adoptium](#)

Licenses:
Apache License, Version 2.0
Eclipse Distribution License 1.0 (BSD)
Eclipse Public License 2.0
— (Secondary) GNU General Public License, version 2 with OpenJDK Assembly Exception
— (Secondary) GNU General Public License, version 2 with the GNU Classpath Exception

The content of this open source project is received and distributed under the license(s) listed above. Some source code and binaries may be distributed under different terms. Specific license information is provided in file headers and in NOTICE files distributed with the project's binaries.

Latest Releases:
From July 7th, 2021 to July 20th, 2021

Name	Date	Review
2021.07.20	2021-07-20	
2021.07.07	2021-07-07	

Active Member Companies:
Member companies supporting this project over the last three months.

PROJECT LINKS
[Website](#)

SLSA
Eclipse Temurin™ declares compliance with SLSA level 2

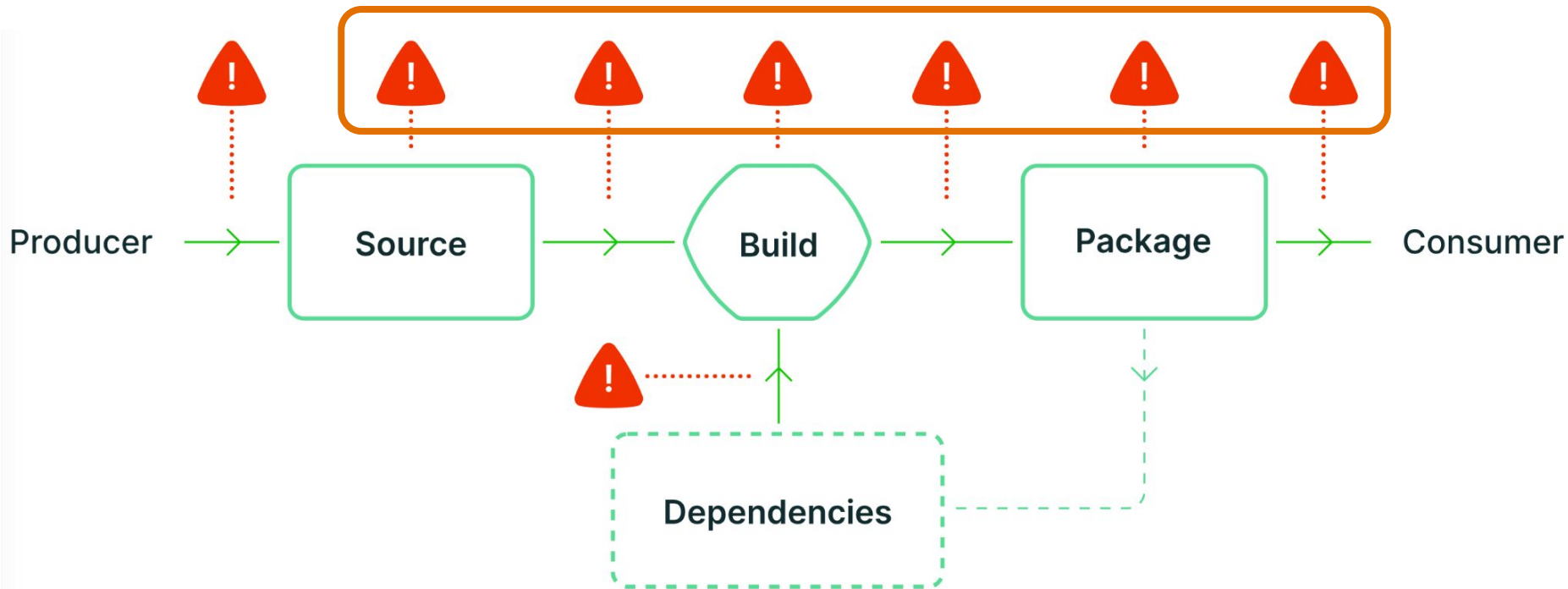
TEMURIN
by ADOPTIUM

RELATED PROJECTS

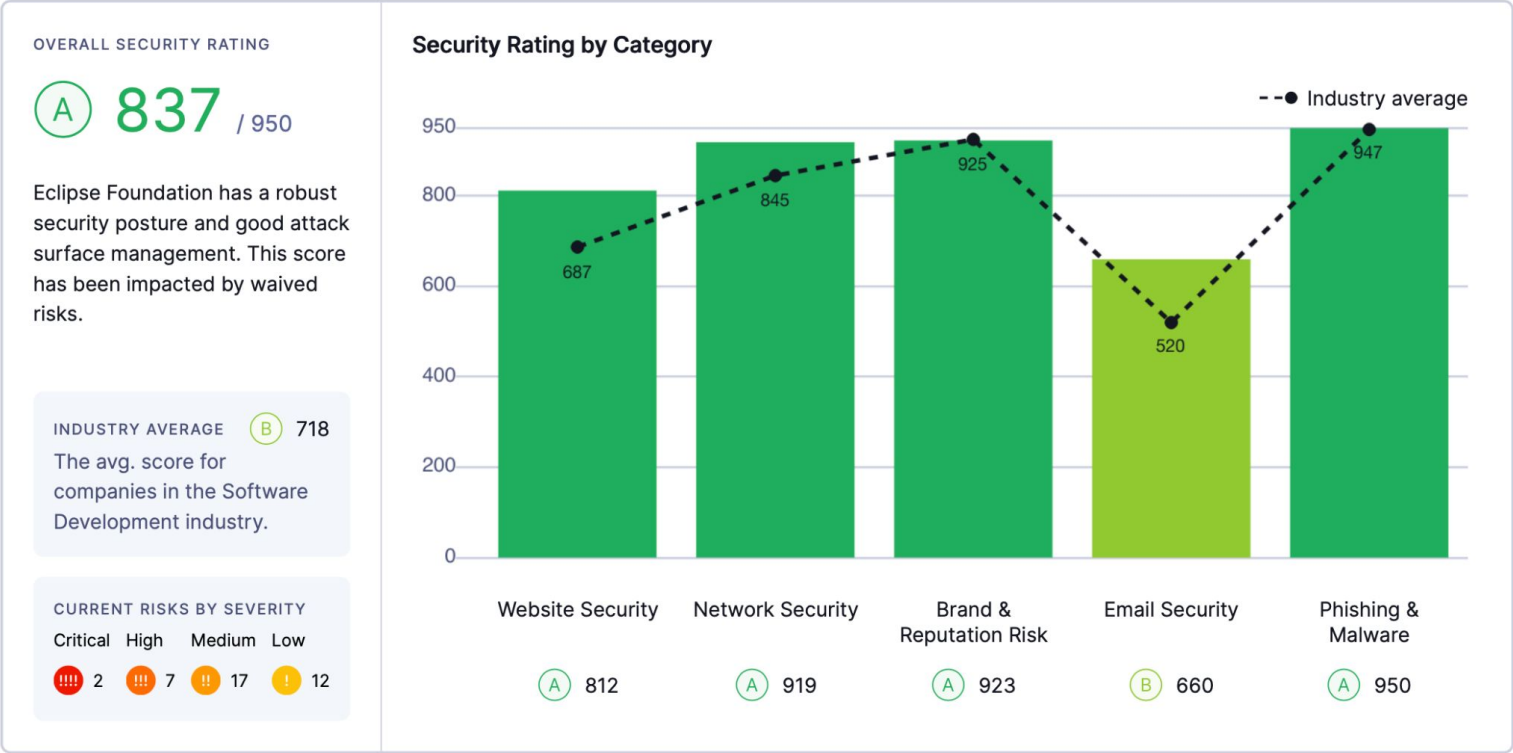


<https://slsa.dev>

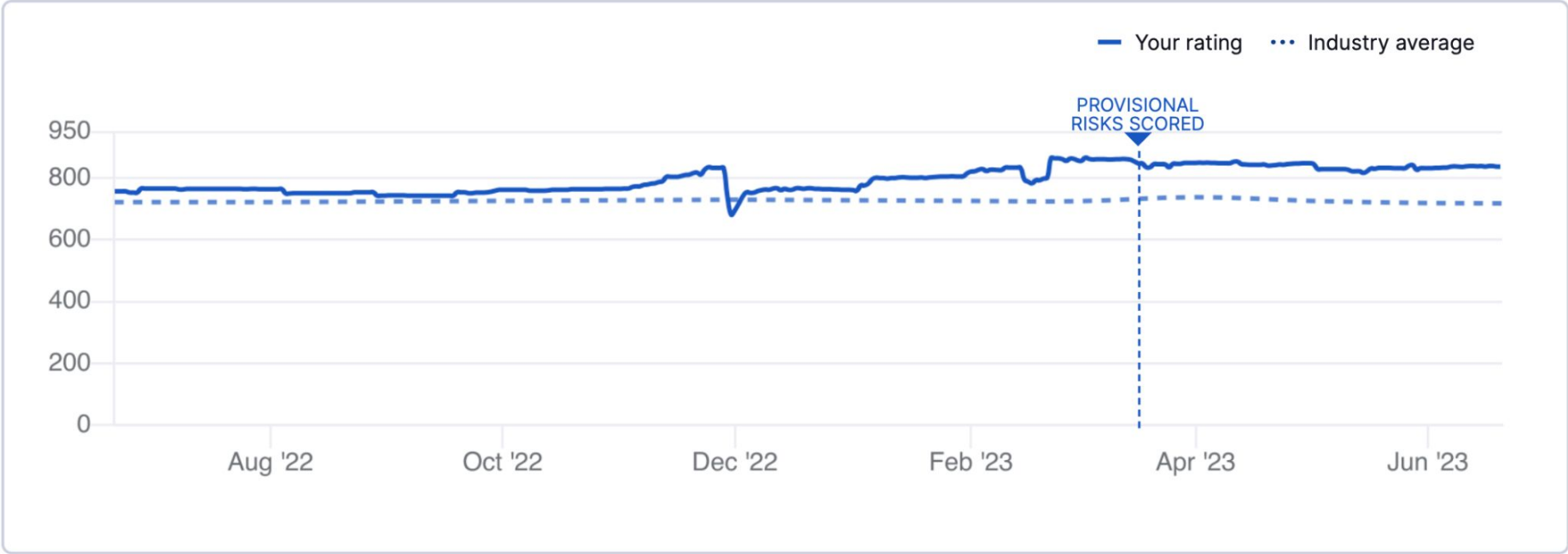
Software Supply Chain & Threats



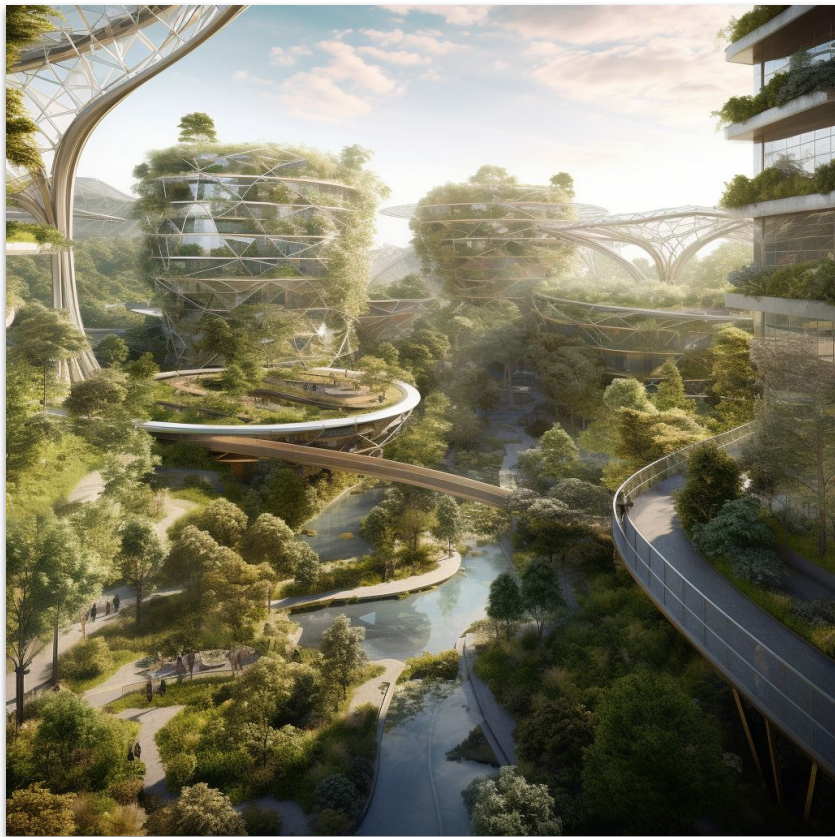
Infrastructure Hardening



Infrastructure Hardening



What's next?



- Harden infrastructure
 - Secret management, traceability, auditability, monitoring
 - accounts.eclipse.org (e.g., 2FA)
- Dependency management
 - Vulnerabilities tracking
 - Opportunity for a joined effort with legal's team
- Harden distribution
 - Reconsidering the approach to download.eclipse.org



ECLIPSE
CYBER RISK
INITIATIVE



Projects Working Groups Members M

Home / About Us / Eclipse Working Groups / Eclipse Foundation Cyber Risk Initi...

Eclipse Foundation Cyber Risk Initiative Concept

This document is intended to motivate discussions around creating and funding a Cyber Risk Initiative Working Group at the Eclipse Foundation. It is our hope that it will be a call to action to bring Eclipse Foundation members and stakeholders together to discuss collective action to improve the cyber resilience of the Eclipse Foundation projects, community, and infrastructure.

Open source supply chain security is top of mind across the entire Information and Communication Technologies (ICT) industry today. The motivations are well documented and outside the scope of this document. However, it is clear that the Eclipse Foundation, its community, its projects, and its industry collaborations all have a strong motivation to be leaders in advocating and implementing security best practices. Our members, adopters, users, and stakeholders all seek to reduce their security risks to the fullest extent possible. As demonstrated by draft legislation from a number of jurisdictions, governments expect industry to act to improve software security.

One thing that is clear, however, is that simply putting the entire burden of added security work on the shoulders of our committers and project leaders is not an option. This topic needs to be addressed by services provided by the Eclipse Foundation to our project community or it will fail. Without strong support in terms of release and build engineering, tooling, and education, developers simply do not have the time, interest, or skills necessary to be responsible for implementing security best practices. It is equally true that security, and particularly supply chain security, requires a programmatic approach. Security is not an attribute that you simply add to existing software.

The Eclipse Foundation believes a strategic investment is needed to significantly enhance our security processes across all aspects of our operations, both internally and with our projects. Achieving this goal cannot be done by simply shifting current resources; rather, it will require additional resources from its membership and stakeholders. We have made progress in building staff capacity and initiating key security-related initiatives, and now our goal is to sustain and potentially accelerate these efforts, ensuring continued growth and improvement in our security processes and infrastructure. Even in the most optimistic of scenarios, assisting our 400+ projects to improve security will be a long and laborious process.

Based on the above, the Eclipse Foundation is proposing to establish a Cyber Risk Initiative to fund, collaborate on, and prioritize enhancements to our security-related processes and infrastructure. The goal is to raise €1.5M in funding for a minimum of each of the next three years in order to achieve these improvements. The establishment and prioritization of the initiatives using those funds will be the responsibility of the working group itself, although some thoughts are outlined below.



Projects Working Groups Members More

Log in Manage Cookies

Download

Home / About Us / Eclipse Working Groups / Eclipse Cyber Risk Initiative Worki...

Eclipse Cyber Risk Initiative Working Group Charter

Draft - Not Yet Approved

Version 0.1 - Revision history at end of document

Vision and Scope

The mission of the Eclipse Cyber Risk Initiative Working Group ("ECRI") is to ensure the security and integrity of Eclipse Foundation's community, projects, systems, and data by implementing the industry's best practices and standards for software production, risk management and incident response. Our goal is to ensure that our community, projects, systems and data are protected against potential threats and vulnerabilities, and that we are able to respond promptly and effectively in the event of a security incident.

Our vision is to have the Eclipse Foundation be recognized across the industry as a leading security organization, known for our ability to proactively identify and mitigate risks, and effectively respond to incidents. We strive to create a culture of security and to be a trusted advisor to our stakeholders on all matters related to security. This includes providing guidance and expertise on security best practices to ensure that the Eclipse community, projects, systems, and data are protected to the highest degree possible.

Based on the above, the Eclipse Cyber Risk Initiative Working Group ("ECRI") will fund, collaborate on, and prioritize enhancements to our security-related processes and infrastructure. The prioritization of security-related initiatives will be the responsibility of the working group Steering Committee via its annual strategy setting and program plan processes.

The Working Group will:

- Drive improvements to the Eclipse Foundation's security policies and processes for all projects.
- Drive improvements to the Eclipse Foundation's infrastructure that supports our open source projects.
- Drive improvements to the security of our projects by providing services to them including assistance in supporting our improved processes, external security audits, and dependency analyses to mitigate for known vulnerabilities.
- Help our committers and contributors improve their skills through training.
- Promote the Eclipse project community's ability to deliver supply chain secure open source components, frameworks, and runtimes.

Eclipse Working Groups

Explore Working Groups

About Working Groups

5 Reasons to Collaborate

Related Links

Working Group Process

Working Group Operations

Working Group Development
Effort Guidelines

Member Funded Initiatives

<https://www.eclipse.org/org/workinggroups/eclipse-cyber-risk-charter.php>

<https://www.eclipse.org/org/workinggroups/eclipse-cyber-risk-concept.php>





Thank you!