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
Cybercrime: World’s 3rd Largest Economy

1. USA
2. China
3. Anonymous

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

Global Supply Chain
What is a Software Supply Chain?

https://slsa.dev/
Where are the Threats?

https://slsa.dev/
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

Calendar No. 677

117th CONGRESS
2d Session

S. 4913

[Report No. 117-278]

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Sponsored by Senator Schumer, February 21, 2022

Mr. Fenn (for himself and Mr. Fieneman) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs.

December 19, 2022

Reported by Mr. Fenn, with amendments.

... (text continues through and beyond the page margin) ...

A BILL

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Securing Open Source Software Act of 2022".
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
OSS Platform

Products Added Value

Infrastructure for Open Collaboration
Ecosystem Development
Community Governance & Processes
IP Management & Licensing
Supply Chain Security
Security - Community Effort

- Shared Cost
- Define services and processes
- Regulation Compliance across jurisdictions
- Create a Culture and Skillset
Software Supply Chain & Threats
Security Audits

Security Assessment of OSTIF’s Eclipse Application with Threat Model

Eclipse JKube
Security Assessment
15 May, 2023

Prepared for:
Marc Hunt San Felice
The Eclipse Foundation
Organised by the Open Source Technology Improvement Fund, Inc.

Prepared by: Artur Cygan and Emilio López
Vulnerability reports management

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 members of 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 list 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

Eclipse Foundation Security Team

Staff Members

Mikaël Barbero
- mbarbero@eclipse.org
- mbarbero@github.com
- @mbarbero@github.com
- @mbarbero@hashyderm.io
- mikael.barbero@hashyderm.io
- mikael.barbero@eclipse-foundation.org
- 39AF 56A7 46AB 3E21 4FDE 9E6E E1E5 5F0B 59A4 24FB

Tiago Lucas
- tiagolucas@eclipse.org
- tiagolucas@github.com
- @tiagolucas@github.com
- tiagolucas@whitehat.com
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.

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 *

---

### 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.
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...

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!

https://gitlab.eclipse.org/eclipsefdn/security/otterdog
In one sentence!

Command line tool to administer GitHub resources, such as organization and repository settings, as code.
Software Supply Chain & Threats

- Producer
- Source
- Build
- Package
- Dependencies
- Consumer

⚠️⚠️⚠️⚠️⚠️
## SLSA

- Set of incrementally adoptable guidelines for supply chain security

### Table: SLSA Requirements

<table>
<thead>
<tr>
<th>Implementer</th>
<th>Requirement</th>
<th>Degree</th>
<th>L1</th>
<th>L2</th>
<th>L3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Producer</td>
<td>Choose an appropriate build platform</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Follow a consistent build process</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Distribute provenance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Build platform</td>
<td>Provenance generation</td>
<td>Exists</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Authentic</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Unforgeable</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Isolation strength</td>
<td>Hosted</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Isolated</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SLSA

$ 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/206071d5ca7a2346e4db4dcbb19a648c7f13b4957e655f4382b735894059bd199

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
Eclipse Temurin™

Overview

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 TOX-tested for general use across the Java ecosystem.

JOIN US! To join the project, please sign up 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 licenses listed above. Some source code and binaries may be distributed under different terms. Specific license information is provided in the headers and is NOTED files distributed with the project’s licenses.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021.07.20</td>
<td>2021-07-20</td>
<td></td>
</tr>
<tr>
<td>2021.07.07</td>
<td>2021-07-07</td>
<td></td>
</tr>
</tbody>
</table>

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

https://slsa.dev
Software Supply Chain & Threats
Infrastructure Hardening

OVERALL SECURITY RATING

A 837 / 950

Eclipse Foundation has a robust security posture and good attack surface management. This score has been impacted by waived risks.

INDUSTRY AVERAGE B 718

The avg. score for companies in the Software Development industry.

CURRENT RISKS BY SEVERITY

Critical High Medium Low

2 7 17 12

Security Rating by Category

Website Security 812 A
Network Security 919 A
Brand & Reputation Risk 923 A
Email Security 660 B
Phishing & Malware 950 A

Industry average
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 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 of the scope of this document. However, it is clear that the Eclipse Foundation, its community, its projects, and its industry collaborators 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 committees 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.

Thank you!