



What's new for open source and security?

You need to improve the security posture of your project!

Mikaël Barbero
Head of Security



**NORDIC SOFTWARE
SECURITY SUMMIT**

THE SOFTWARE SECURITY REGULATION REVOLUTION

The largest Open Source Foundation from Europe

Global presence,
reach, and reputation



Eclipse Foundation is One of the World's Largest Open Source Organizations





Eclipse Foundation is the best place for consuming and developing secure Open Source Software

Advocate for the projects you're passionate about.
Encourage them to join Eclipse Foundation's secure ecosystem
– whether they're your own projects or those you rely on

Why Open Source Security Matters?

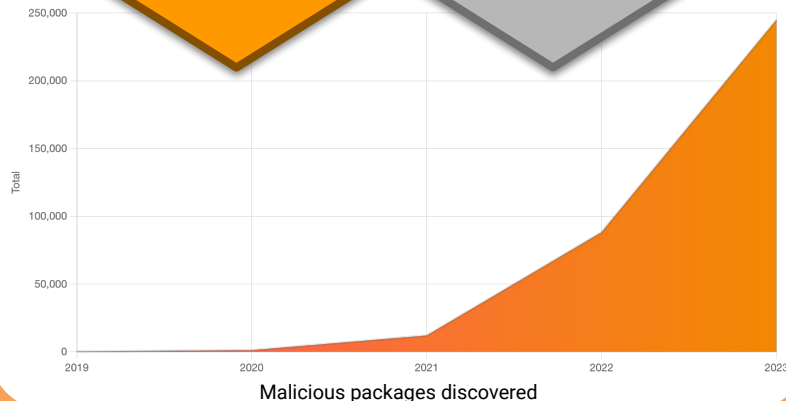
Maven Central / Java Ecosystem

96%

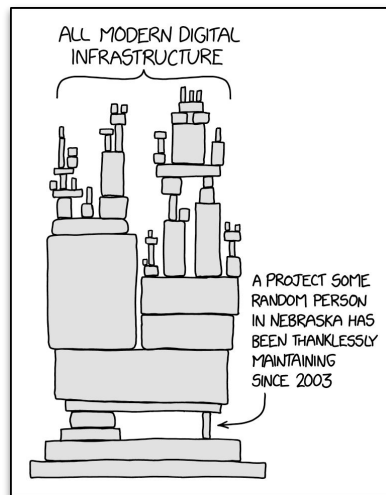
of vulnerable
downloaded releases
had a remediated
version available

12%

downloads served
has a known security
vulnerability



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



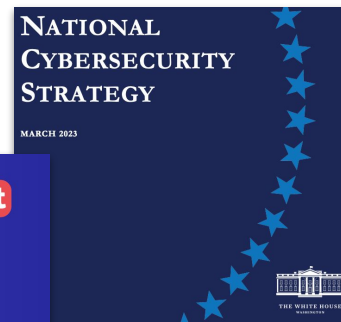
<https://xkcd.com/2347/>

79%

of professionals working
with OSS find
maintaining security
policies or compliance
challenging

2024 State of Open Source Report
(OpenLogic, OSI, Eclipse Foundation)

<https://newsroom.eclipse.org/news/announcements/2024-state-open-source-report-now-available>



We complement the OpenSSF



OpenSSF

OPEN SOURCE SECURITY FOUNDATION



The **OpenSSF Alpha-Omega** project is backing our initiative to kickstart this effort

We embody their vision of what an Open Source Software Foundation should do

Leading Partner

Board Level Priority
for the Entire
Organization

Dedicated Team
driving Culture,
Processes, and
Solutions

Eclipse Foundation Security Overview

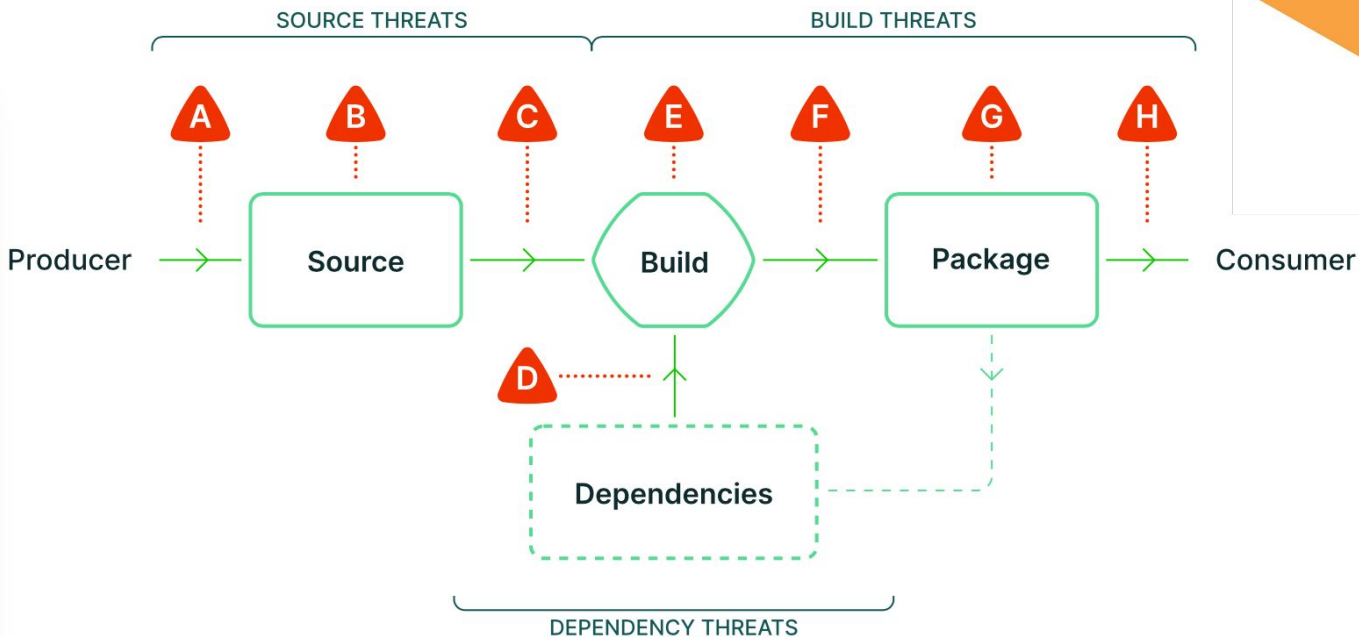
Members and Projects Dashboard / Control Plane

Comprehensive
Set of Security
Practices and
Services

Project and
Developer
Mentoring and
Support

Regulatory
Compliance
Assistance

Security Experts Team



SOURCE THREATS

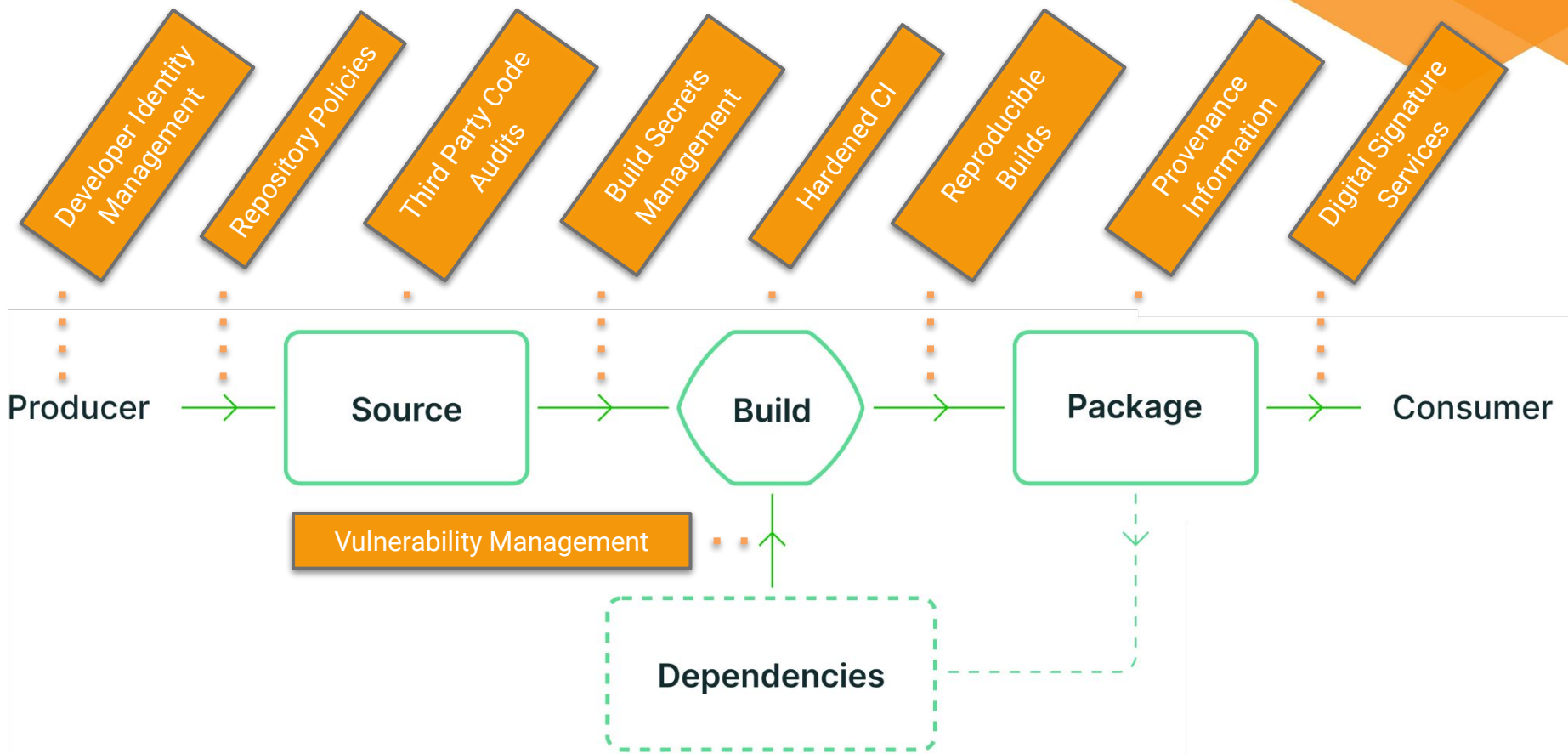
- A** Submit unauthorized change
- B** Compromise source repo
- C** Build from modified source

DEPENDENCY THREATS

- D** Use compromised dependency

BUILD THREATS

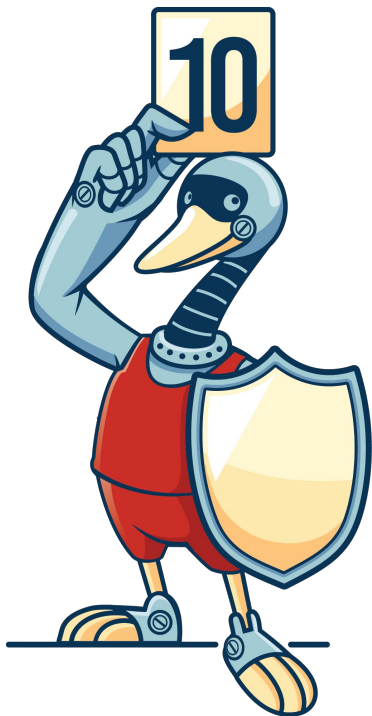
- E** Compromise build process
- F** Upload modified package
- G** Compromise package registry
- H** Use compromised package



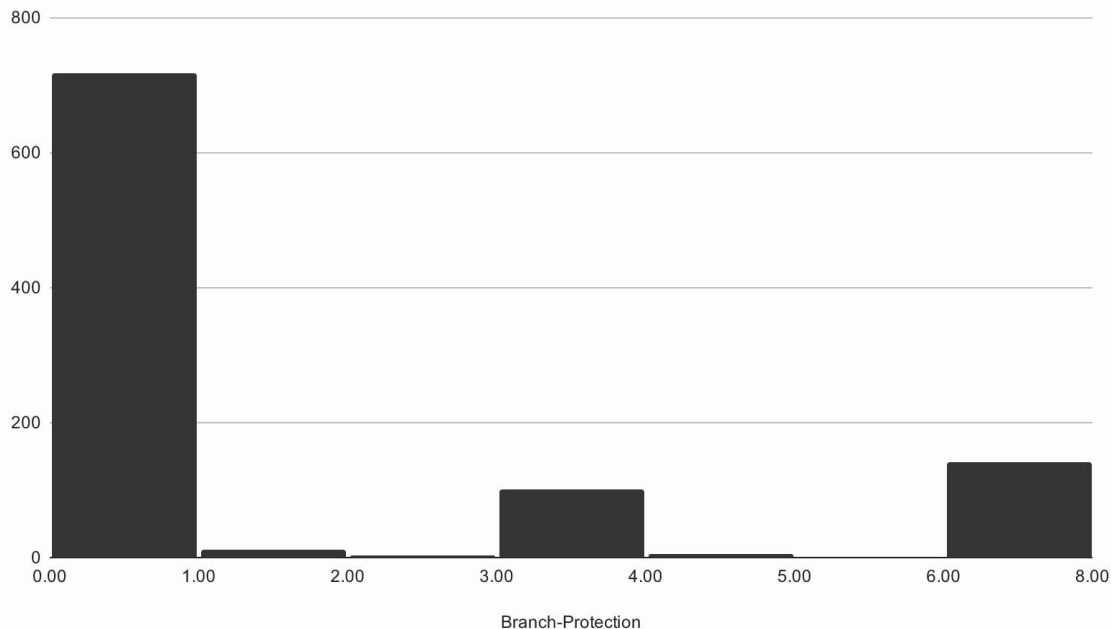
Enforcing MFA for developers



Scorecard: how it started



Histogram of Branch-Protection



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

Taming the Octocat, at our scale!

200+

GitHub Organizations...
and counting!

2000+

GitHub Repositories...
and counting!



...how it's going!



github.com/eclipse-csi/otterdog

eclipse-csi / otterdog

< Code Issues (28) Pull requests Discussions Actions Wiki Security Insights Settings

otterdog (Public)

Edit Pins Unwatch (4) Fork (2) Starred (5)

main 2 Branches 5 Tags

Go to file Add file <> Code

netomi	fix: use pagination when retrieving all branches of a repo	c791105 · 1 hour ago	681 Commits
.github/workflows	churn: support none as version fragment to increase	last month	
docker	churn: fix license header	3 weeks ago	
docs	feat: support private vulnerability reporting (#205)	last month	
examples	Use std function for example default config.	10 months ago	
otterdog	fix: use pagination when retrieving all branches of a repo	1 hour ago	
tests	Scoped commands (#215)	2 weeks ago	
.dockerignore	churn: generate static content using vite (#207)	last month	
.flake8	Fix flake issues with tests folder, add tests to inspection.	last year	
.gitignore	churn: generate static content using vite (#207)	last month	
.pre-commit-config.yaml	churn: update dash hook	3 weeks ago	
.readthedocs.yaml	churn: update build for readthedocs	2 months ago	
CHANGELOG.md	fix: use pagination when retrieving all branches of a repo	1 hour ago	
CODE_OF_CONDUCT.md	Add code of conduct	3 months ago	

About

OtterDog is a tool to manage GitHub organizations at scale using a configuration as code approach. It is actively used by the Eclipse Foundation to manage its numerous projects hosted on GitHub.

otterdog.readthedocs.org

python security supply-chain
asyncio configuration-as-code
github-config

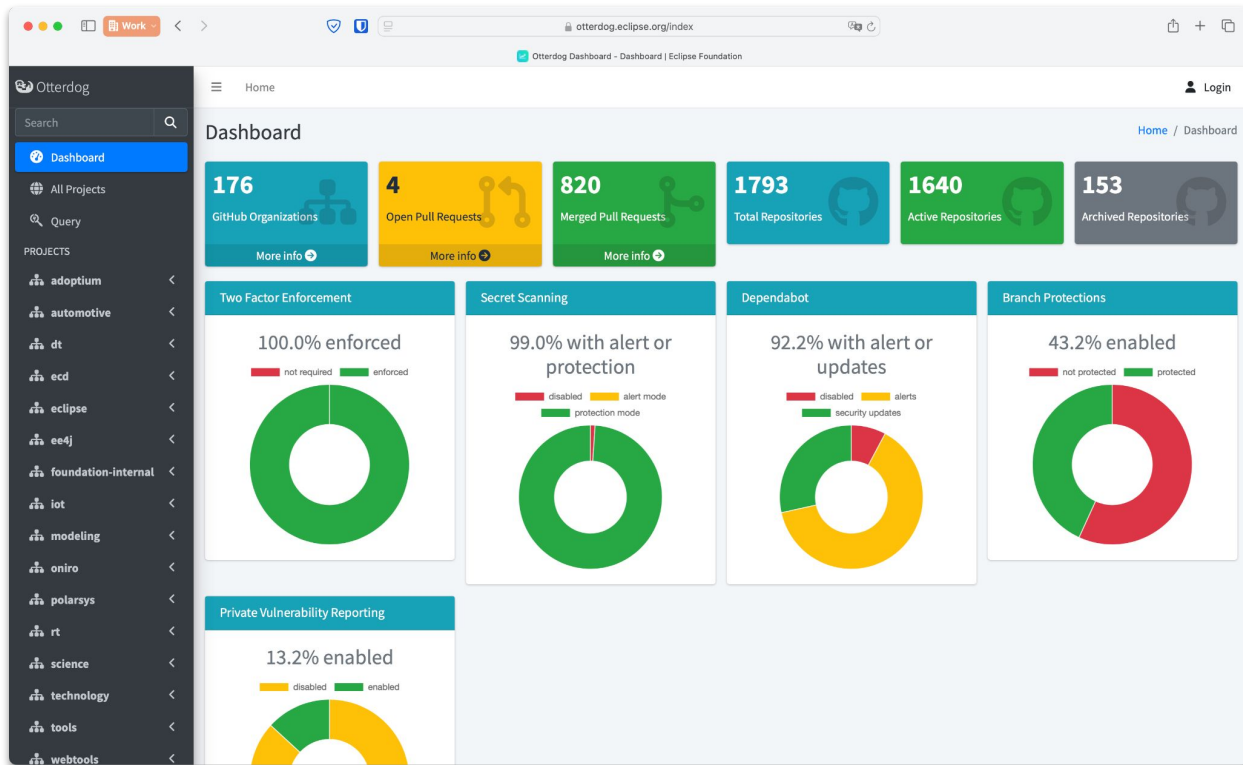
Readme
EPL-2.0 license
Code of conduct
Activity
Custom properties
5 stars
4 watching
2 forks
Report repository

Releases (5)

<https://github.com/eclipse-csi/otterdog>




...how it's going!



<https://github.com/eclipse-csi/otterdog>

Vulnerability Management



 Security Handbook Developer [Vulnerability Management](#) References

[Home](#) > [Vulnerability Management](#) > [Best Practices Related to Embargoes](#)

Best Practices Related to Embargoes


This document presents recommendations on handling embargoes by Eclipse Foundation projects. In general, projects should adhere to the [Eclipse Foundation Vulnerability Reporting Policy](#); this document provides additional guidelines and best practices when handling embargoes. Each project might decide to act differently if the situation, and security of their users, requires this.

Readers of this document should be familiar with terms and definitions of the [Eclipse Foundation Development Process](#) and the [Eclipse Foundation Vulnerability Reporting Process](#). Please review them if needed.

What is an embargo?

An *embargo* is a term used to name the period of time from the moment a vulnerability is disclosed to the vendor, to the moment it is made public by announcement of the CVE number (Common Vulnerabilities Enumeration), and

On this page

 Security Handbook Developer [Vulnerability Management](#) References

[Home](#) > [Vulnerability Management](#) > [Security Advisories](#)

Security Advisories

Security advisories allow projects to communicate security information to users. They contain a description of a vulnerability (or a class of vulnerabilities) and solutions to follow. They usually contain information on which versions of the product are affected and which ones contain a fix; they mention possible workarounds if available.

This document presents recommendations on handling advisories by Eclipse Foundation projects. In general, projects should adhere to the [Eclipse Foundation Vulnerability Reporting Policy](#); this document provides additional guidelines and best practices. Each project might decide to act differently if the situation, and security of their users, requires this.

Readers of this document should be familiar with terms and definitions of the [Eclipse Foundation Development Process](#) and the [Eclipse Foundation Vulnerability Reporting Process](#). Please review them if needed.

What is the difference between a CVE entry and a security advisory?

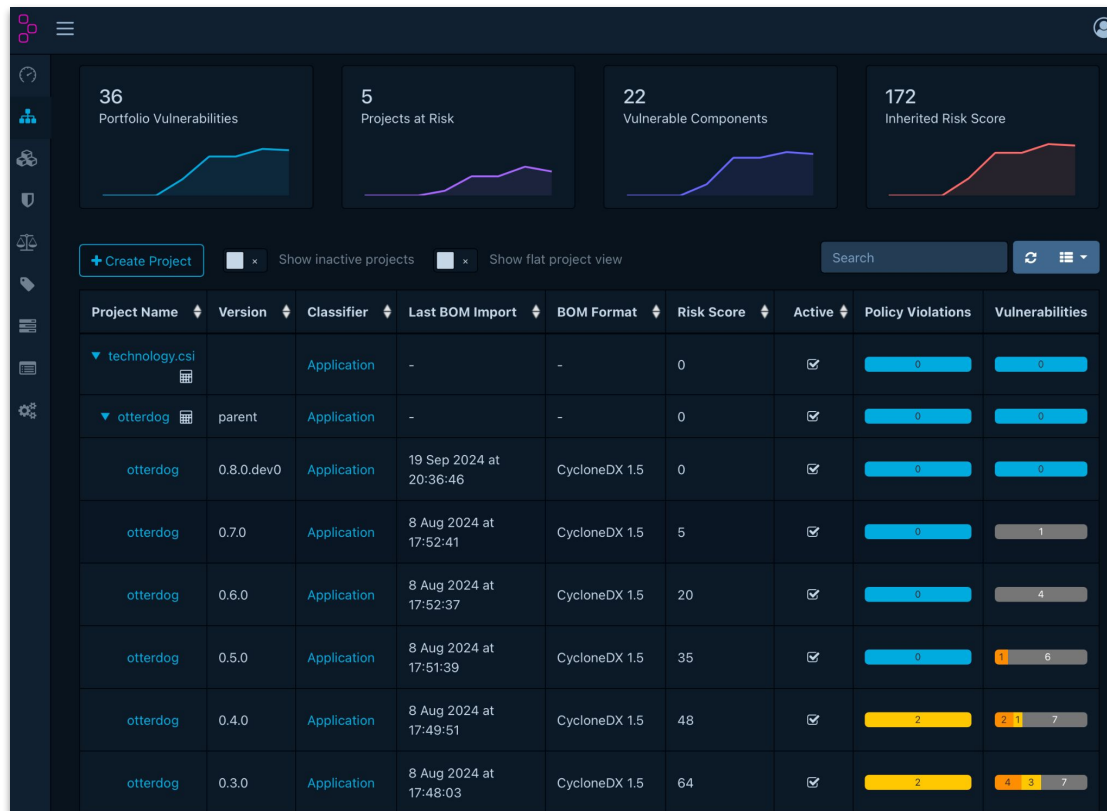
On this page

- What is the difference between a CVE entry and a security advisory?
- Process
- Pre-advisories and advisories without fixes
- Reference content
- Technical means
- Standard formats
- Frequently asked question

[Edit on GitHub](#)
[Show Source](#)

<https://eclipse-csi.github.io/security-handbook>

Vulnerability Management



Security Features

Source Threats Mitigations

- **Enhanced Developer Identity Verification**
 - Implement **Multi-factor Authentication** to ensure secure code access
 - Enforce **Cryptographic Commit Signing** to verify integrity and origin of code
- **Code Audits by Independent Third Parties**
 - In-depth reviews of codebase
 - In-house security expertise
- **Repository Configuration Policies – OtterDog**
 - **Branch Protection rules** to safeguard against unauthorized changes
 - Mandate **Code Reviews** to enhance code quality and security
 - Strict **vetting of Third-Party integration** to ensure compliance with security policies
- **Secrets Protection**
 - Adopt a **Zero Trust approach** to minimize insider threats
 - Proactive **Leak Scanning** to detect and address potential exposures early
- **Proactive Vulnerability Management**
 - Facilitate communication between vulnerability reporters and developers
 - **CVE Numbering Authority**
 - Training, Material, and Support for responsible and coordinated vulnerability disclosure processes

Build Threats Mitigations

- **Enhanced CI/CD Security:** on secured, dedicated infrastructure and on third-party CI/CD services
 - Conduct **comprehensive audits** of CI/CD pipelines
 - Leverage **support from a Release Engineering team** for best practices
 - Generate **software provenance records** compliant with SLSA standards
- **Achievable Reproducible Builds**
 - Provide guidelines and support for consistent build processes
- **Strengthened Infrastructure Security**
 - **Continuous monitoring** to evaluate external security threats
 - **Intrusion detection systems** to identify potential breaches
- **Digital Signature Solutions**
 - Support for **platform-specific digital signatures**
 - Efficient certificate management processes
- **Robust Package Management:** Integrate and support third-party package registries for broader software distribution
 - Also maintain an on-premises, security-enhanced package registry

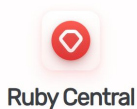
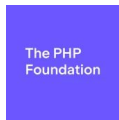
Dependencies Threats Mitigations

- **Automated SBOM Generation:** Facilitate the creation of Software Bill of Materials (SBOMs) to improve transparency and tracking of all software components.
- **Policy Compliance Scans in CI/CD Pipelines**
 - **License Compliance:** Ensure all dependencies comply with legal and regulatory license requirements.
 - **Vulnerability Detection:** Identify and mitigate security vulnerabilities within dependencies.
 - **Malicious Dependency Detection:** Screen for and prevent the inclusion of compromised or malicious dependencies.
- **Ongoing Vulnerability Monitoring:** Continuously monitor dependencies in existing releases for newly discovered vulnerabilities, ensuring long-term security and compliance.
- **Proactive Harmful Dependency Prevention:** Utilize caching proxies for external repositories, integrated with a dependency firewall, to proactively block the use of harmful dependencies, enhancing security and reliability

Regulatory Compliance Assistance

- **Simplify and Optimize Compliance Adherence**
 - Assist in understanding and documenting project compliance with policy requirements, provide attestations where required
 - Continuous tracking and monitoring of progress in meeting policy requirements
 - Automate alerts to address any lapses in regulatory obligations
- **Focusing on Key Regulations**
 - EU's Cyber Resilience Act (CRA), focusing on Annex I's requirements
 - US's M-22-18, directed by Executive Order (EO) 14028
- **Active Engagement in Public Policy**
 - In Brussels and Washington, D.C.

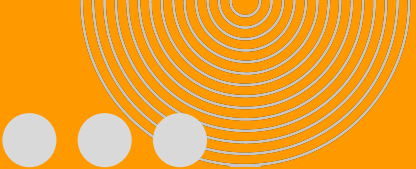
Regulatory Compliance Assistance



<https://orcwg.org>

Eclipse Foundation Security Benefits

- **Mitigate Risks in Open Source Collaboration and Consumption**
 - Reduce the regulatory risks associated with collaborating on and relying upon open source projects
- **Help Developers Provide more secure open source projects**
 - Have team of security professionals guide and help projects with services, tools and expertise.
- **Simplify Compliance Adherence**
 - Ease the complexity of adhering to regulatory requirements with expert guidance and tools



**Eclipse Foundation is the leading
Foundation providing security as a
first class service to developers,
projects, and members**

Services & Tools
Regulatory Compliance Assistance
Project and Developer Guidance and Mentoring