



# 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**

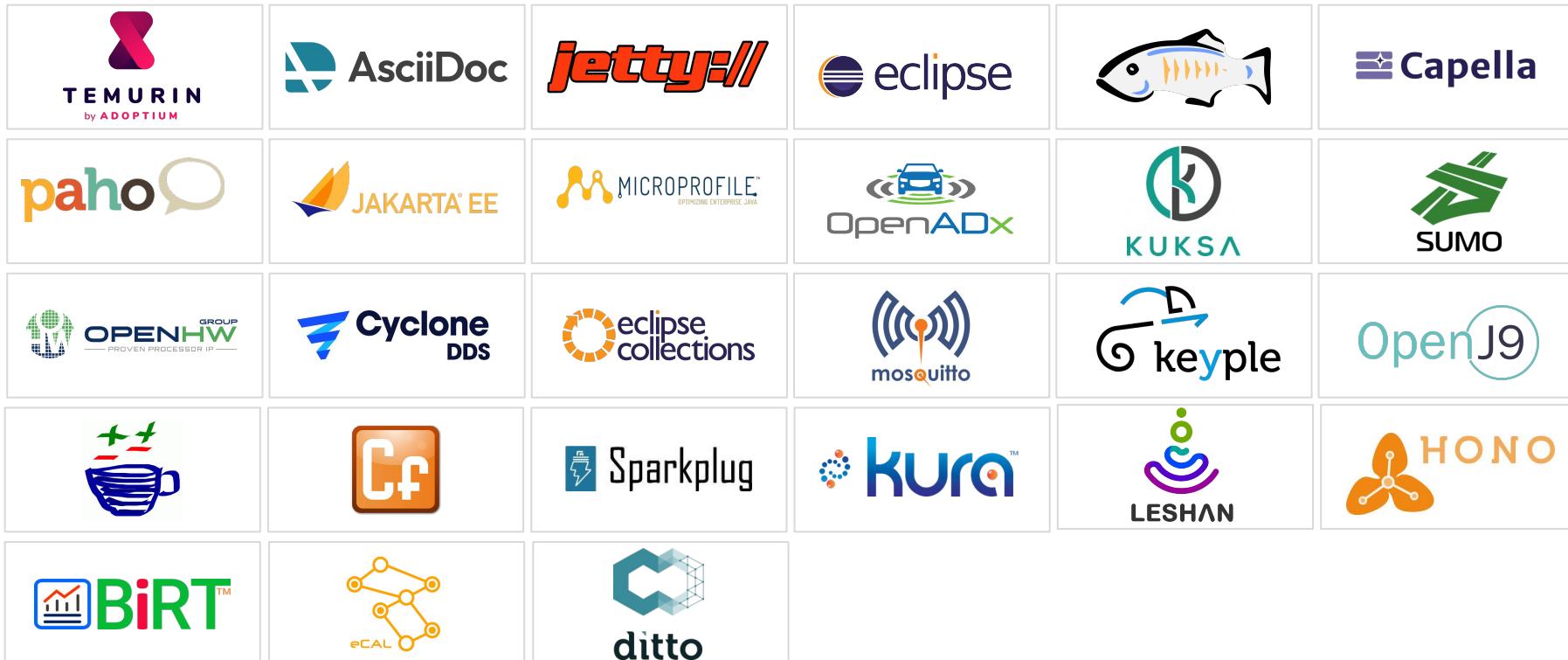
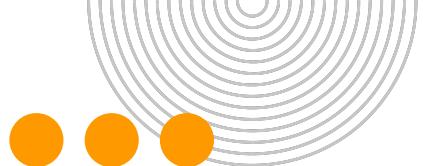
THE SOFTWARE SECURITY REGULATION REVOLUTION

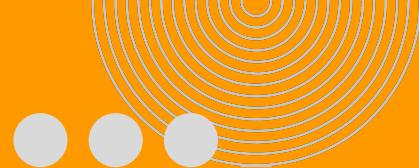
# The largest Open Source Foundation from Europe

Global presence,  
reach, and reputation



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



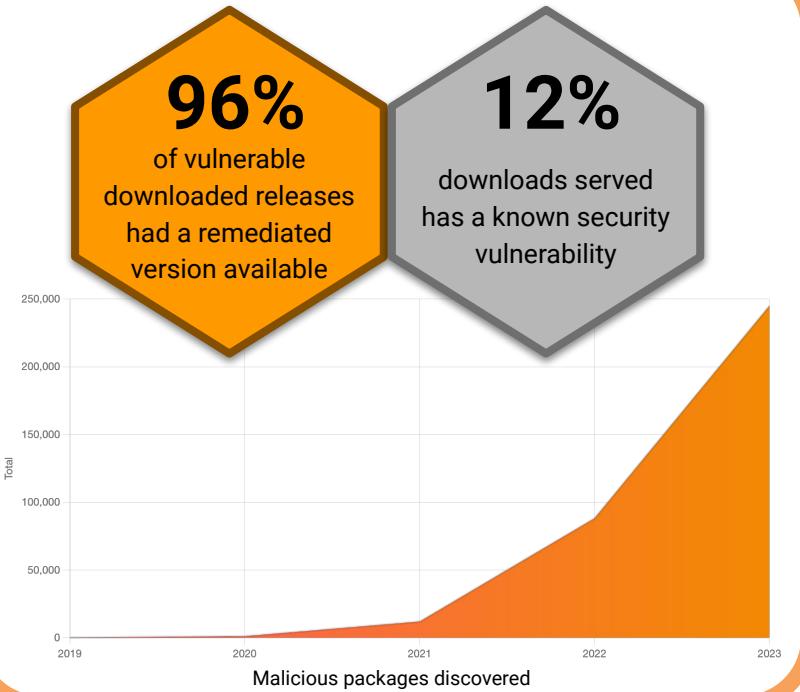


# Eclipse Foundation is the best place for consuming and developing secure Open Source Software

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



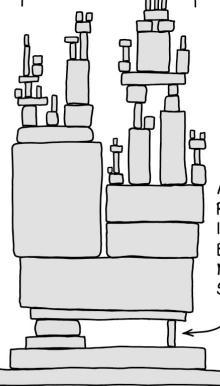
**96%**

of vulnerable  
downloaded releases  
had a remediated  
version available

**12%**

downloads served  
has a known security  
vulnerability

ALL MODERN DIGITAL  
INFRASTRUCTURE



<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>

NATIONAL  
CYBERSECURITY  
STRATEGY

MARCH 2023

EU Cyber Resilience Act



For safer & more secure  
digital products

#DigitalEU #CyberSecEU

ECLIPSE  
FOUNDATION

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

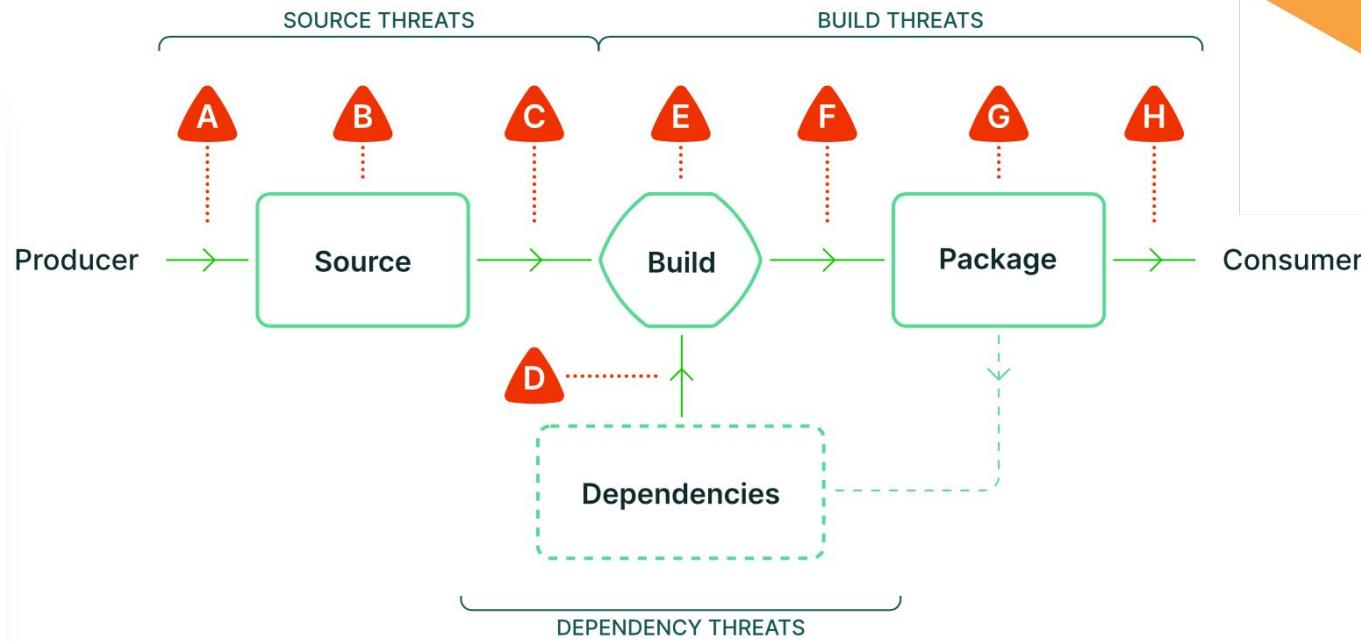
## Members and Projects Dashboard / Control Plane

Comprehensive Set of Security Practices and Services

Project and Developer Mentoring and Support

Regulatory Compliance Assistance

Security Experts Team



#### SOURCE THREATS

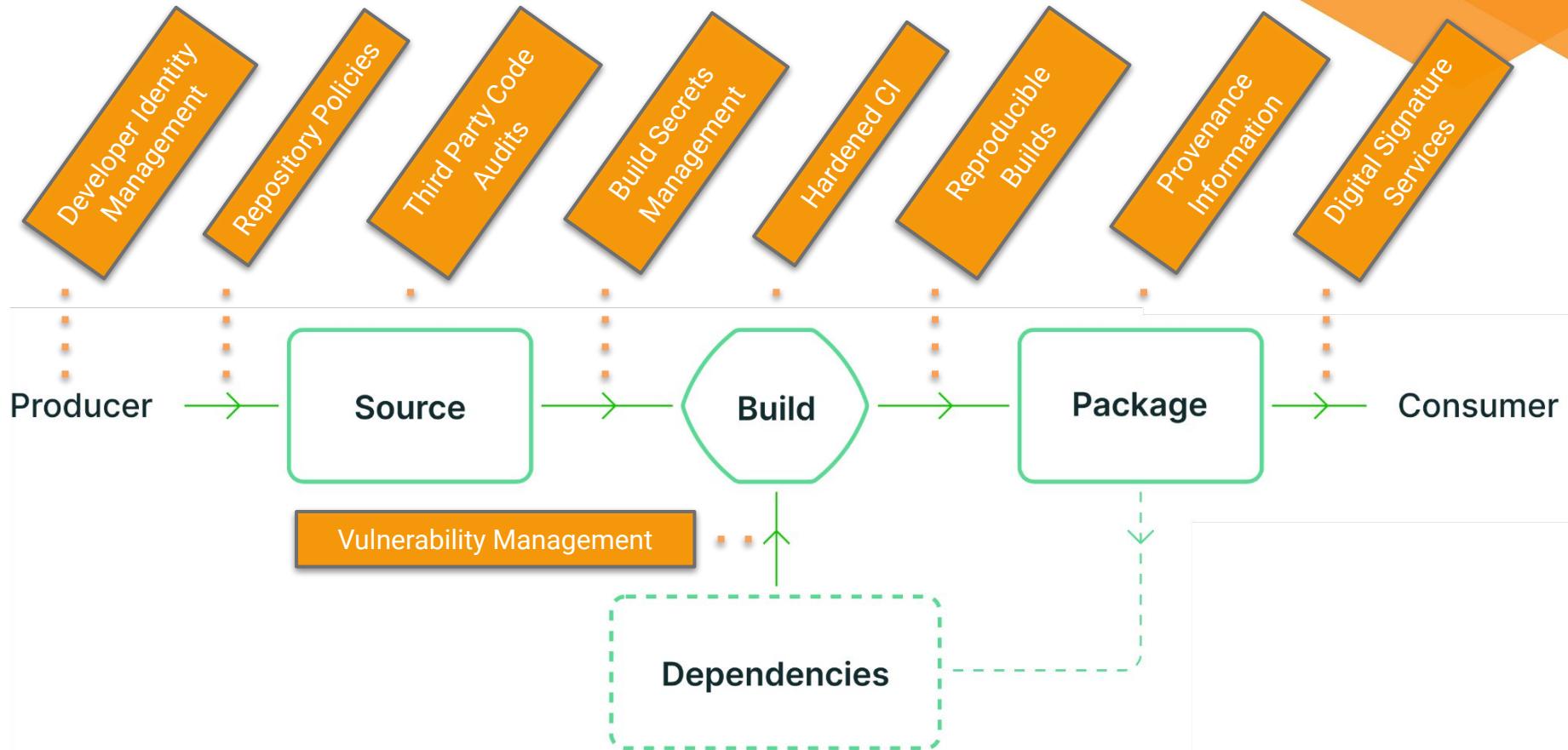
- A Submit unauthorized change
- B Compromise source repo
- C Build from modified source

#### DEPENDENCY THREATS

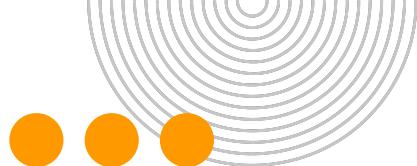
- D Use compromised dependency

#### BUILD THREATS

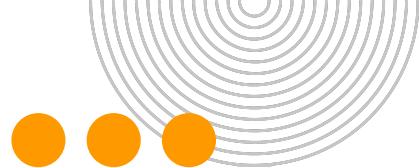
- E Compromise build process
- F Upload modified package
- G Compromise package registry
- H Use compromised package



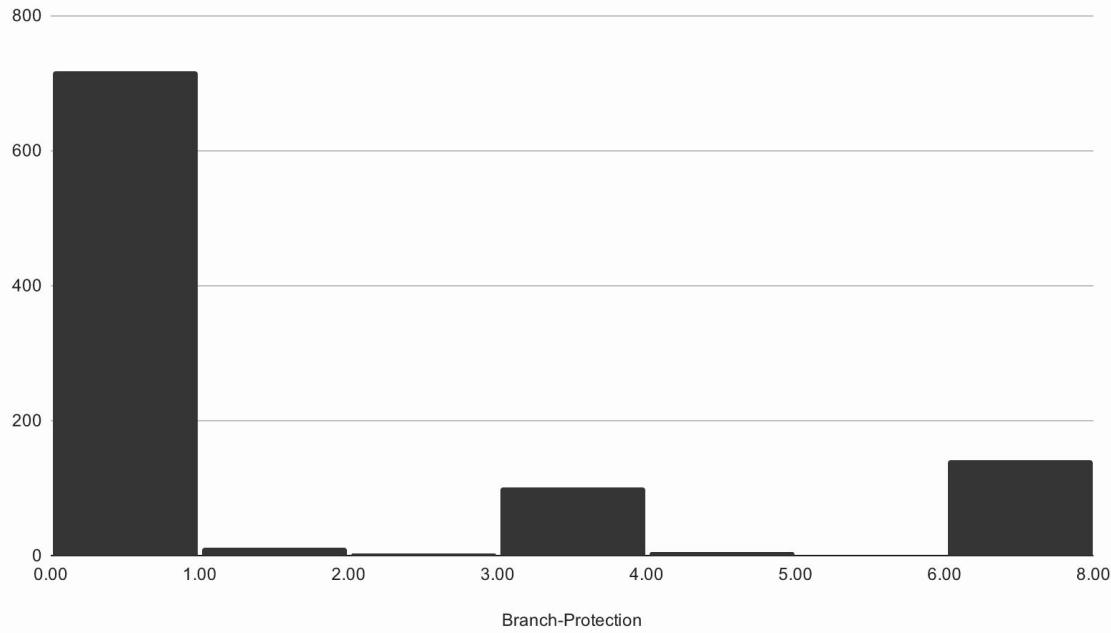
# Enforcing MFA for developers



# Scorecard: how it started

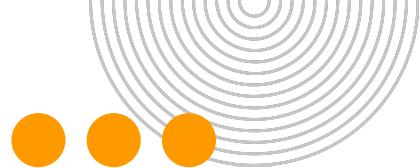


Histogram of Branch-Protection



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

# Taming the Octocat, at our scale!

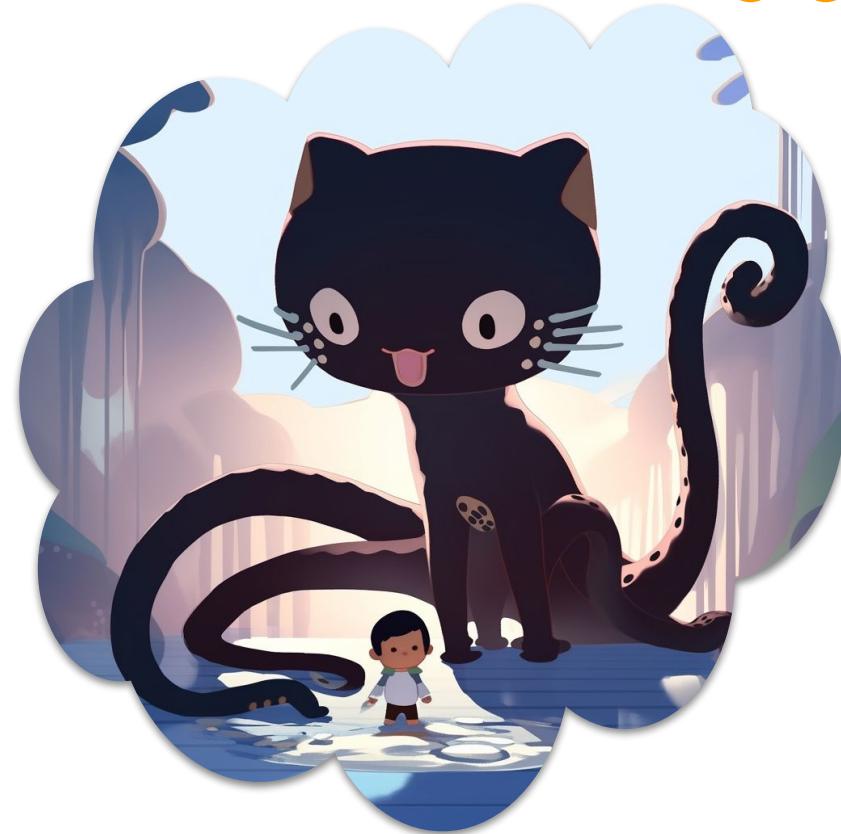


**200+**

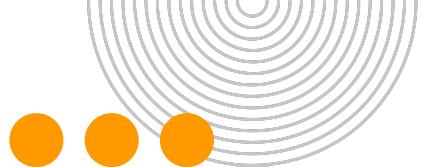
GitHub Organizations...  
and counting!

**2000+**

GitHub Repositories...  
and counting!



# ...how it's going!

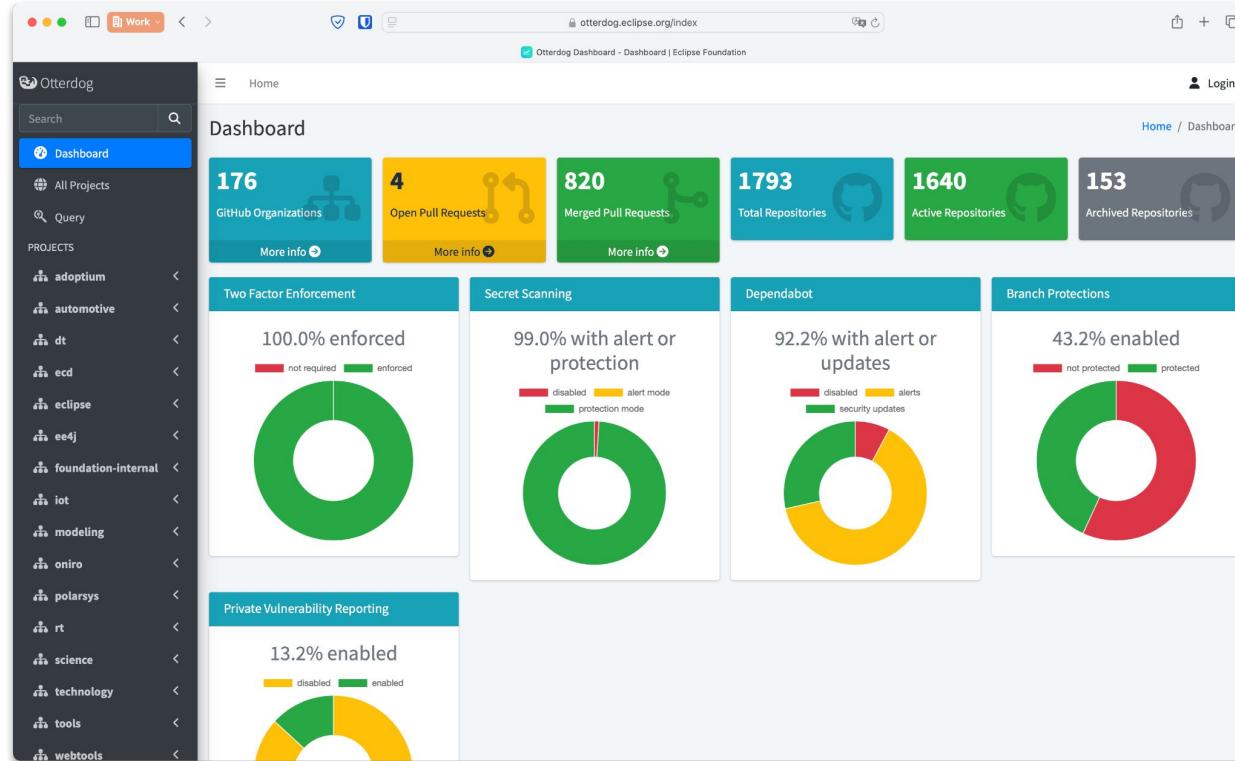
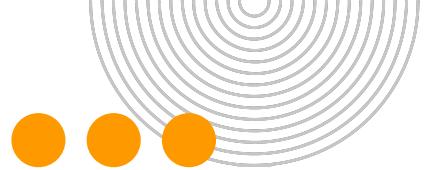


Screenshot of the GitHub repository page for `eclipse-csi/otterdog`. The repository has 2 branches and 5 tags. The main branch contains several commits from various authors, including `netomi`, `.github/workflows`, `docker`, `docs`, `examples`, `otterdog`, `tests`, `.dockercfgignore`, `.flake8`, `.gitignore`, `.pre-commit-config.yaml`, `.readthedocs.yaml`, `CHANGELOG.md`, and `CODE_OF_CONDUCT.md`. The repository is public and has 681 commits. It includes links to `otterdog.readthedocs.org` and various GitHub files like `Readme`, `EPL-2.0 license`, `Code of conduct`, `Activity`, `Custom properties`, and `Report repository`.

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

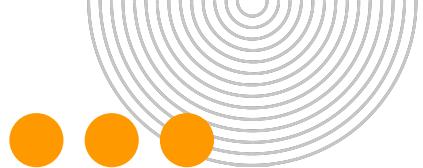


# ...how it's going!



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

# Vulnerability Management



## Section Navigation

[Best Practices Related to Embargoes](#)

Security Advisories

🏠 > Vulnerability Management > Best...

## 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. It also refers to the announcement of the CVE number (Common Vulnerabilities Enumeration), a unique identifier for the vulnerability.

## Section Navigation

[Best Practices Related to Embargoes](#)

[Security Advisories](#)

🏠 > 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.

## 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

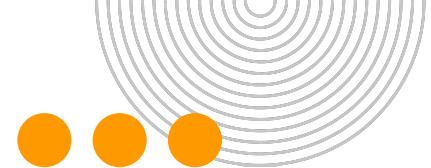
Frequently asked question

>Edit on GitHub

Show Source

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

# Vulnerability Management



36 Portfolio Vulnerabilities

5 Projects at Risk

22 Vulnerable Components

172 Inherited Risk Score

+ Create Project Show inactive projects Show flat project view Search

Project Name	Version	Classifier	Last BOM Import	BOM Format	Risk Score	Active	Policy Violations	Vulnerabilities
technology.cs		Application	-	-	0	<input checked="" type="checkbox"/>	0	0
otterdog	parent	Application	-	-	0	<input checked="" type="checkbox"/>	0	0
otterdog	0.8.0.dev0	Application	19 Sep 2024 at 20:36:46	CycloneDX 1.5	0	<input checked="" type="checkbox"/>	0	0
otterdog	0.7.0	Application	8 Aug 2024 at 17:52:41	CycloneDX 1.5	5	<input checked="" type="checkbox"/>	0	1
otterdog	0.6.0	Application	8 Aug 2024 at 17:52:37	CycloneDX 1.5	20	<input checked="" type="checkbox"/>	0	4
otterdog	0.5.0	Application	8 Aug 2024 at 17:51:39	CycloneDX 1.5	35	<input checked="" type="checkbox"/>	0	6
otterdog	0.4.0	Application	8 Aug 2024 at 17:49:51	CycloneDX 1.5	48	<input checked="" type="checkbox"/>	2	7
otterdog	0.3.0	Application	8 Aug 2024 at 17:48:03	CycloneDX 1.5	64	<input checked="" type="checkbox"/>	2	7

# Security Features

Source Threats Mitigations	Build Threats Mitigations	Dependencies Threats Mitigations
<ul style="list-style-type: none"><li>● <b>Enhanced Developer Identity Verification</b><ul style="list-style-type: none"><li>○ Implement <b>Multi-factor Authentication</b> to ensure secure code access</li><li>○ Enforce <b>Cryptographic Commit Signing</b> to verify integrity and origin of code</li></ul></li><li>● <b>Code Audits by Independent Third Parties</b><ul style="list-style-type: none"><li>○ In-depth reviews of codebase</li><li>○ In-house security expertise</li></ul></li><li>● <b>Repository Configuration Policies – OtterDog</b><ul style="list-style-type: none"><li>○ <b>Branch Protection rules</b> to safeguard against unauthorized changes</li><li>○ Mandate <b>Code Reviews</b> to enhance code quality and security</li><li>○ Strict <b>vetting of Third-Party integration</b> to ensure compliance with security policies</li></ul></li><li>● <b>Secrets Protection</b><ul style="list-style-type: none"><li>○ Adopt a <b>Zero Trust approach</b> to minimize insider threats</li><li>○ Proactive <b>Leak Scanning</b> to detect and address potential exposures early</li></ul></li><li>● <b>Proactive Vulnerability Management</b><ul style="list-style-type: none"><li>○ Facilitate communication between vulnerability reporters and developers</li><li>○ <b>CVE Numbering Authority</b></li><li>○ Training, Material, and Support for responsible and coordinated vulnerability disclosure processes</li></ul></li></ul>	<ul style="list-style-type: none"><li>● <b>Enhanced CI/CD Security:</b> on secured, dedicated infrastructure and on third-party CI/CD services<ul style="list-style-type: none"><li>○ Conduct <b>comprehensive audits</b> of CI/CD pipelines</li><li>○ Leverage <b>support from a Release Engineering team</b> for best practices</li><li>○ Generate <b>software provenance records</b> compliant with SLSA standards</li></ul></li><li>● <b>Achievable Reproducible Builds</b><ul style="list-style-type: none"><li>○ Provide guidelines and support for consistent build processes</li></ul></li><li>● <b>Strengthened Infrastructure Security</b><ul style="list-style-type: none"><li>○ <b>Continuous monitoring</b> to evaluate external security threats</li><li>○ <b>Intrusion detection systems</b> to identify potential breaches</li></ul></li><li>● <b>Digital Signature Solutions</b><ul style="list-style-type: none"><li>○ Support for <b>platform-specific digital signatures</b></li><li>○ Efficient certificate management processes</li></ul></li><li>● <b>Robust Package Management:</b> Integrate and support third-party package registries for broader software distribution<ul style="list-style-type: none"><li>○ Also maintain an on-premises, security-enhanced package registry</li></ul></li></ul>	<ul style="list-style-type: none"><li>● <b>Automated SBOM Generation:</b> Facilitate the creation of Software Bill of Materials (SBOMs) to improve transparency and tracking of all software components.</li><li>● <b>Policy Compliance Scans in CI/CD Pipelines</b><ul style="list-style-type: none"><li>○ <b>License Compliance:</b> Ensure all dependencies comply with legal and regulatory license requirements.</li><li>○ <b>Vulnerability Detection:</b> Identify and mitigate security vulnerabilities within dependencies.</li><li>○ <b>Malicious Dependency Detection:</b> Screen for and prevent the inclusion of compromised or malicious dependencies.</li></ul></li><li>● <b>Ongoing Vulnerability Monitoring:</b> Continuously monitor dependencies in existing releases for newly discovered vulnerabilities, ensuring long-term security and compliance.</li><li>● <b>Proactive Harmful Dependency Prevention:</b> Utilize caching proxies for external repositories, integrated with a dependency firewall, to proactively block the use of harmful dependencies, enhancing security and reliability</li></ul>

# 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



The image shows the Eclipse Foundation website's header for the Open Regulatory Compliance Working Group. It features a dark blue background with a wavy pattern. At the top, the Eclipse Foundation logo is on the left, and a navigation menu with links to "About", "Membership", "Participate", and "Participation and Membership FAQ" is on the right. In the center, the text "OPEN REGULATORY COMPLIANCE WORKING GROUP" is displayed in large, bold, white capital letters. Below this, a smaller text block reads: "Key Stakeholders From Industry and Open Source Communities Are Collaborating to Support Compliance With Government Regulations, Ensuring The Continued Use and Advancement of Open Source Through the Software Supply Chain." At the bottom, there are two orange call-to-action buttons: "Get Involved" and "Learn More".

<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