FINOS

Fintech
Open Source
Foundation

Pan-PMC Monthly Meeting

FINOS Team

November 19, 2019

Agenda

I. **Vulnerabilities Responsible Disclosure and WhiteSource Automated Scanning - Mao**
   - Security vulnerabilities responsible disclosure
   - Submit a vulnerability & manage a FINOS project
   - WhiteSource automated scanning
   - WhiteSource rollout plan

II. **FINOS Project Lifecycles Review - Gab**
   - Criteria
   - Stewardship and Responsibilities
   - Archiving

III. **Community Building - Gab and James**
   - Building Sustainable "public task tracking" in github and marking "good first issues" as a unified practice to garner "organic" contribution.

IV. **FINOS Q4 Board Meeting Re-Cap - Gab and Rob**
   - The Future of Programs as a Construct

V. **OSSF - Last call!**
   - Get ready for an amazing day tomorrow!

I. Vulnerabilities Responsible Disclosure and WhiteSource Automated Scanning

James/Mao

Security vulnerabilities responsible disclosure

*A set of **rules and policies** established by FINOS to manage the lifecycle of security incidents across FINOS projects, aimed to guarantee...*

1. **Discretion** for new and ongoing development activity around security vulnerabilities that haven't been published yet
2. **Transparency and guidance** around security vulnerabilities that have been identified, patched and released as new versions

https://finosfoundation.atlassian.net/wiki/spaces/FINOS/pages/1230176257/Security+vulnerabilities+responsible+disclosure

Submit a vulnerability

Unless not publicly available (via project's GitHub issues), you can:

1. **Identify the FINOS Project** related to the security vulnerability and its related Program
2. **Identify the private PMC email address** (on FINOS Wiki), fallback to help@finos.org
3. **Submit the description** of the vulnerability via email

Manage a FINOS project

1. **Managing new vulnerabilities**, consisting of triaging to accept the issue, work on a fix, apply it to released versions, publishing new binaries and CVE info (as GitHub Issue)
2. **Collecting project CVE list** - using GitHub Issues and label `security vulnerability`
3. **Automating security vulnerabilities**, by using WhiteSource to automatically scan third party libraries for CVE.

WhiteSource automated scanning

Features

1. All PRs and commits are automatically scanned
2. Email sending can be configured (by the FINOS Infra team) for new vulnerabilities
3. Supports 20 different dependency resolution frameworks
4. Supports scanning only for runtime dependencies (ie ignoring `devDependencies`), which is what FINOS requires
5. False positives can be mitigated by excluding files from scanning (similar to what `.gitignore` does)
6. Can be enabled at GitHub org level

https://finosfoundation.atlassian.net/wiki/spaces/FDX/pages/1129283585/WhiteSource+for+GitHub.com

WhiteSource rollout plan

19 Nov.	New feature alert at Pan PMC meeting
20 Nov.	FINOS and WhiteSource presenting at OSSF
Dec.	Blogpost on www.finos.org
Dec.	Start enabling WhiteSource automated scanning to ***trending projects***, one at the time. FINOS Infra team will reach out to project leads and help setting up the bot.
Jan.	Enable scanning at org level (across all FINOS hosted projects)
Jan.	Socialize results with pmcs@finos.org and FINOS community

Trending Projects

- ***cla-bot (pilot in progress)***
- datahelix
- openfin-react-hooks
- plexus-interop
- finos-plexus.github.io
- perspective
- cloud-service-certification
- kdb
- greenkey-discovery-sdk
- greenkey-asrtoolkit

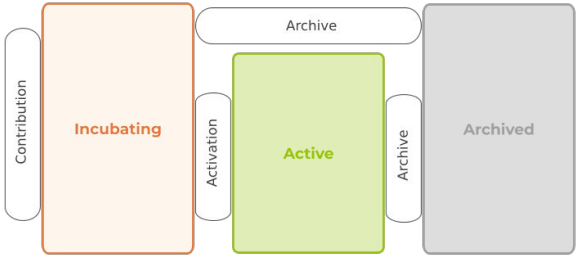
II. FINOS Project Lifecycles Review

Gab

II. FINOS Project Lifecycle Review

https://finosfoundation.atlassian.net/wiki/spaces/FINOS/pages/75530756/Project+Lifecycle

- What is the Project lifecycle?
  1. Incubating
  2. Active
  3. Archived



- Why does it exist?
  1. First and foremost, a concise way to signal Project maturity to consumers
  2. Secondly, helps contributors understand where to focus their efforts
  3. Provide a recommended “meta-recipe” for successful OSS projects

- Projects should always be striving towards “Activation”

II. Recent lifecycle changes

- On 07/24, Board approved:
  - Renamed “Released” state into “Active” state
  - Quantitative criteria for Incubating (contribution criteria)
  - Quantitative criteria for Active (activation criteria)

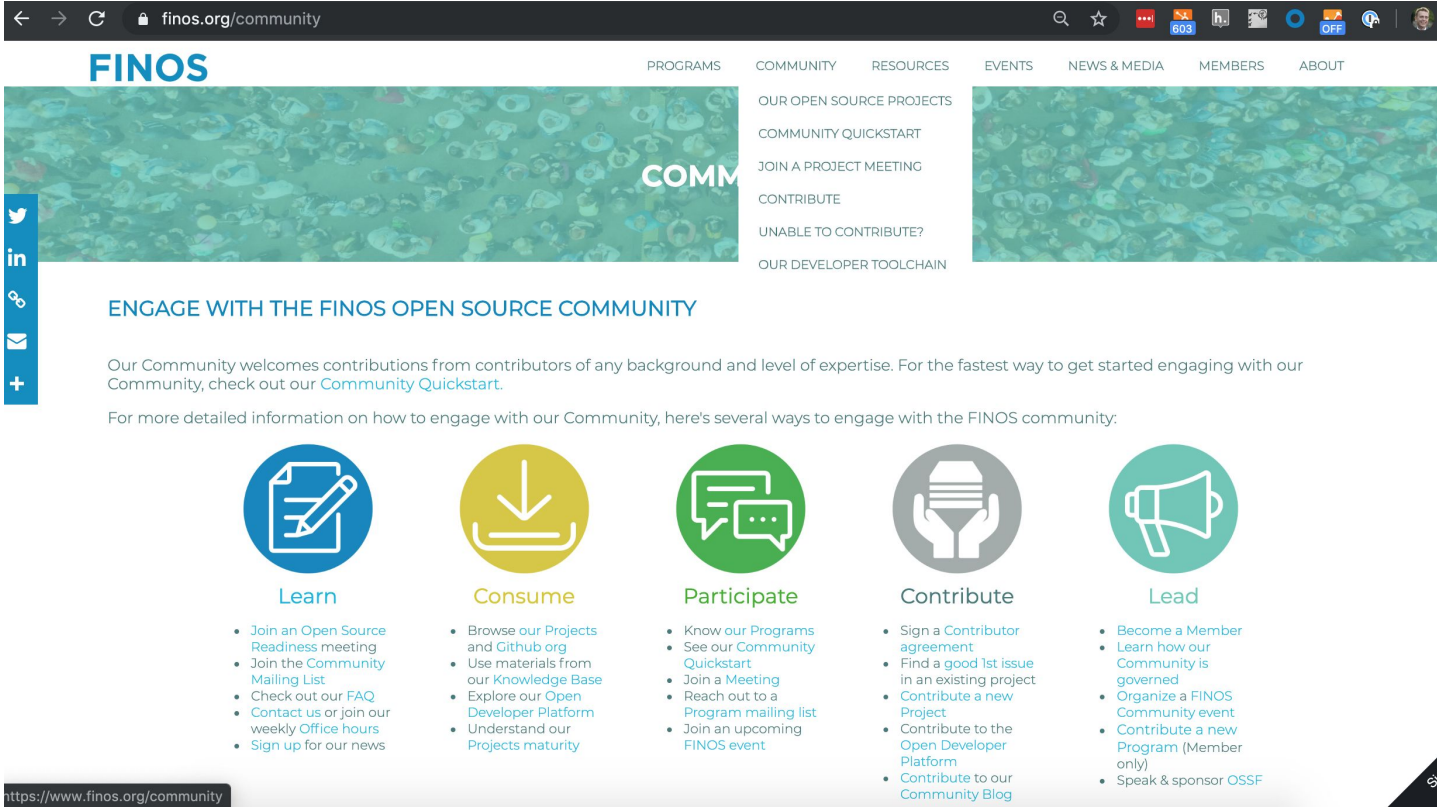
- Stewardship and Responsibilities
  - Based on the criteria, PMCs (currently, more on this later) should approve lifecycle transitions, i.e. explicitly [VOTE] on whether a project is active. Example
  - Along the same lines, inactive Projects should be periodically archived by PMCs (hence the automated monthly reports

- A note on **Archiving:**
  - A Board 2019 KR is to have no projects incubating longer than 1 year. Help us!

III. Community Building

James & Gab

Understanding (and modeling) the Contributor journey



https://www.finos.org/community

III. Community Building

- Public Task Tracking
  - Good First Issues

- It’s not just about putting the code out there
  - The FINOS team can help, but it’s largely about how you help us simplify the onramp by maintaining public task lists elaborating “what help you need” - we can’t do that for you!
  - “They can’t hear you on mute” - great presentation from Don Raab (Java champion and BNYM MD)

- Join Office Hours weekly with James, and develop a plan to grow contribution or adoption

IV. FINOS Q4 Board Meeting Re-cap

Rob & Gab

Objectives

1. Simplify a governance which has turned out to be burdernning

2. Drive focus from the FINOS team and Member engagement Community on high value efforts

The Gap

Programs were introduced to federate responsibility

PMCs are in charge of nurturing their own Projects through the lifecycle

Programs are supposed to consolidate common activities around a theme/business problem

Software and Standard Projects are all treated similarly under our governance

Programs have become a governance overhead for FINOS and PMCs

PMCs are not mature / engaged enough and responsibility falls on FINOS

Programs are hard to understand and create a barrier of entry for new contributors

Software and standard projects require fundamentally different upfront buy-in from Membership to be successful

2020 Governance Refinements proposal

1. **Do away with Programs**
   - Standard and Software Projects will live at top level. They can still be categorized around similar themes and areas of interest in Github (theming / tagging) and other web properties.
2. **Board commitment to Standard Projects**
   - Standard projects require extensive buy-in from the whole industry, so Board is required to approve new standard, requiring at least 5 Member firms to commit an FTE before standard effort is started.
3. **FINOS approval role in Software Projects**
   - Based on the recently approved Lifecycle criteria, the FINOS team can approve new software Projects in the Foundation (in Incubating state)
4. **Board "activates" Projects**
   - Board will be requested to approve transition from Incubating to Active for (software and standard) Projects that demonstrate to have achieved the required maturity.
5. **FINOS clear focus**
   - FINOS focuses on "coaching" Incubating Projects, while focused "marketing" efforts on Active Projects

Benefits

BENEFIT	HOW?
Focus FINOS resources	Marketing focus only for “Active” projects. Coaching / support focus for Incubating”
Reduce contribution friction	FINOS can approve directly in “Incubating” removing need for PMC need for approval
Lessen governance overhead	Remove need for quarterly Program reporting
Avoid starting “abstract” efforts	Initial buy-in from Board on “industry-wide” efforts (e.g. standards) promotes focus on valuable efforts
Drive banks Member engagement	For standards projects, banks SMEs engagement is required from the get-go

A potential timeline

- **19Q4**
  - Refine proposal to remove Programs and simplify governance
  - Socialization with M&G Committee
  - Socialization with Community
- **20Q1**
  - Feedback from Community
  - Board approval
  - Change implementation by FINOS team
- **20Q2**
  - Launch of restructured web properties (wiki, website, etc.)
  - Prime marketing positioning for “Active” projects
  - Work with “Incubating” projects to draw roadmap to activation

IV. FINOS Q4 Board Meeting Re-cap

- The future of Programs as a construct

OPEN SOURCE STRATEGY FORUM 2019

FINOS NYC | NOVEMBER 20TH

https://opensourcestrategyforum.org

FINOS

Fintech
Open Source
Foundation

finos.org