FINOS

Fintech
Open Source
Foundation

Pan-PMC Monthly Meeting

FINOS Team

November 19, 2019

Agenda

I. **Vulnerabilities Scanning Feature from Whitesource - Mao**
   - Security vulnerabilities responsible disclosure
   - Submit a vulnerability & Manage a FINOS project
   - WhiteSource automated scanning
   - WhiteSource rollout plan

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

III. **Community Building**
   - 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

I. Vulnerabilities Scanning Feature from Whitesource

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. **Collecting project CVE list** - using GitHub Issues and label `security vulnerability`
2. **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
3. **Automating security vulnerabilities**, by using WhiteSource to automatically scan third party libraries for CVE.

WhiteSource automated scanning

Features

1. PRs ***and*** commits are continuously 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***
Jan.	Enable scanning at org level (across all FINOS hosted projects)
20 Nov.	Socialize results with pmcs@finos.org and community

Trending Projects

- ***cla-bot (pilot)***
- 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 & James

II. FINOS Project Lifecycles Review

- Criteria
- Stewardship and Responsibilities
- Archiving

III. Community Building

Rob

III. Community Building

- Good First Issues

- Public Task Tracking

IV. FINOS Q4 Board Meeting Re-cap

Rob & Gab

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