OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Quarterly Town Hall Meeting

February 23, 2022

Thank you for joining us today! We will begin at 8:02a PT.

While we wait for everyone to join, please take a moment to do one (or more) of the following:

★ Please add questions using the Zoom Q&A feature
★ Follow us on Twitter: @theopenssf
★ Sign Up for edX training: https://openssf.org/training/courses/
★ Visit the Website! https://openssf.org/

This meeting is being recorded

Antitrust Policy Notice

Linux Foundation meetings **involve participation by industry competitors**, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Code of Conduct

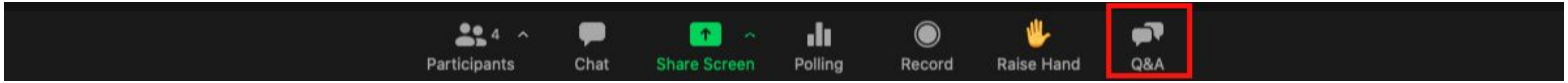
The Linux Foundation and its project communities are **dedicated to providing a harassment-free experience** for participants at all of our events, whether they are held in person or virtually.

All event participants, whether they are attending an in-person event or a virtual event, **are expected to behave in accordance with professional standards**, with both this Code of Conduct as well as their respective employer's policies governing appropriate workplace behavior and applicable laws.

https://lfprojects.org/policies/code-of-conduct/

Housekeeping

Please submit your questions during the meeting by using the Q&A feature on Zoom.



Thank You!

Agenda

- **Welcome**
- **Organizational Update**
- **Selected updates:**
  - **Project Sigstore** (Priya Wadhwa)
  - **Developer Best Practices** (CRob)
  - **Vulnerability Disclosure** (CRob)
  - **Securing Critical Projects** (Amir Montazery)
  - **Alpha-Omega Project** (Michael Scovetta)
  - **Q&A**

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Organizational Update

OpenSSF by the Numbers

Membership (as of Feb 22)

- **Current Active Members: 60**
  23 Premier / 30 General / 7 Associate
- **Just in: Coinbase (Premier)**, Alibaba Cloud (General), Chainguard (General), Cloudsmith (General), Spotify (General), OpenUK (Associate), MITRE (Associate)
- **In-Process:** F5 Networks, Inc. (General), Cycode (General), Checkmarx (General), ISCAS (Associate)

Fundamentals of Developing Secure Software (as of Feb 22)
6,733+

Courses:

- Secure Software Development: Requirements, Design, and Reuse (LFD104x) **3,456 active registrants**
- Secure Software Development: Implementation (LFD105x) **1,638 active registrants**
- Secure Software Development: Verification and More Specialized Topics (LFD106x) **1,639 active registrants**

Community Engagement (as of Feb 22)

- **Mailing Lists:**
  - Main: 866 participants
  - Announce: 546 participants
- **Twitter https://twitter.com/theopenssf**
  - 1,933 Followers

Website
(last 30 days since Feb 22)

- **Site Views:** ~ 22,941 (up from ~ 16,392 Dec-Jan)

Premier Members

1Password
aws
cisco
citi
coinbase
DELL Technologies

ERICSSON
Fidelity INVESTMENTS
GitHub
Google
HUAWEI
intel

IBM
JFrog
JPMorgan Chase & Co.
Meta
Microsoft
Morgan Stanley

ORACLE
Red Hat
snyk
vmware
wipro

General and Associate Members

AccuKnox
aiven
Alibaba Cloud
anchore
apiiro
AURISTOR

BLOCK
BTP
CHAINGUARD
Codethink
cybertrust

deepfence
DeployHub
DTCC
Securing Today. Shaping Tomorrow.
Devgistics
GitLab
Goldman Sachs

Teleport
mongoDB.
nccgroup
NUTANIX.
REVERSING LABS
Spotify

STACKHAWK
Tencent 腾讯
TIDELIFT
WNDRVR
水木羽林
WINGTECHER
cloudsmith

Carnegie Mellon University
LISH
Laboratory for Innovation Science at Harvard

OpenUK
SAFECode

MITRE

Other quick updates:

- New TAC! Congrats to: Abhishek Arya, Aeva Black, Bob Callaway, CRob Robinson, Dan Lorenc, Josh Bressers and Luke Hinds.
- And welcome back to Ian Coldwater as the Security Community Individual Representative to the Governing Board.
- SupplyChainSecurityCon set for June 21-24 in Austin, in parallel with the LF's Open Source Summit.

Update on Project Sigstore

Update on Project Sigstore

- GA Release of Community Instance Coming Soon!
  - Follow along the GitHub Project
- 1.5m log entries!
- 1031 unique GitHub workflows using cosign!
- Support in many major package registries in design phase:
  - PyPI, RubyGems, Maven, Alpine Linux…
- Kubernetes KEP-3031 is aaalllllmmoooossttt done!
  - Kubernetes 1.24 will be signed with sigstore and cosign!

Goals of Sigstore GA

- All sigstore projects (Cosign/Rekor/Fulcio) are 1.0
- Rekor is production ready (99.9% uptime)
- Fulcio is production ready (99.9% uptime)
- We can remove experimental warnings around Fulcio/Rekor usage

Focus Areas

- Infrastructure
- Testing
- Documentation
- Fulcio
- Rekor
- Cosign

Infrastructure / Testing

- Automation!
    - Cutting and Deploying Releases
    - Staging Environment
    - IAM Permissions for the GCP project
- Monitoring
    - Alerts set up via GCP Monitoring
    - Probers set up on Github Actions
- Alerting
    - Alerts from GCP/Github Actions sent to Slack
- Load Testing Fulcio/Rekor
- Comprehensive review of unit/integration tests

Cosign / Rekor / Fulcio

- Removing experimental warnings from cosign
- Adding rate limiting to Rekor and Fulcio
- Adding log sharding to Rekor
- Rekor 1.0
- Fulcio 1.0

Also In Progress...

- A security audit
- Planning an on-call system

How Long Will This Take?

Thank you GA Contributors!

- bobcallaway
- lukehinds
- dlorenc
- haydentherapper
- asraa
- puerco
- cpanato
- k4leung4
- nsmith5
- lkatalin

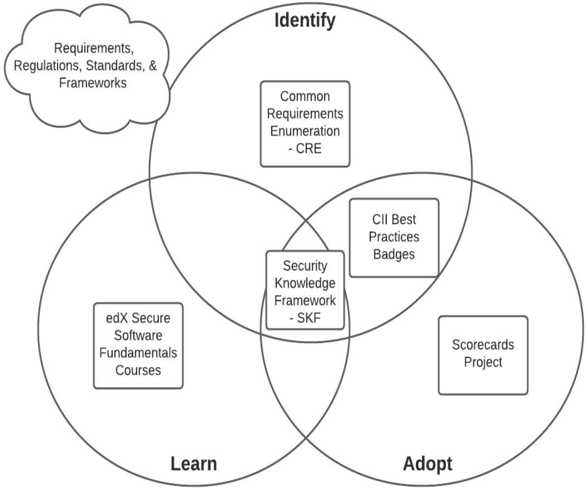
Github Project Planner

Design Doc

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Developer Best Practices

Update on Developer Best Practices


Requirements, Regulations, Standards, & Frameworks
Identify
Common Requirements Enumeration - CRE
CII Best Practices Badges
Security Knowledge Framework - SKF
edX Secure Software Fundamentals Courses
Scorecards Project
Learn
Adopt

- Est. 26Feb2020
- ~33 members with 12 very active
- 6 Core on-going member projects
  - *Common Requirement Enumeration (CRE) Project* (incubating)
    - https://www.opencre.org/
    - Purpose - (Identify) Identify similar requirements in different specifications
  - *Existing Guidelines for Developing and Distributing Secure Software*
    - GitHub Repo
    - Purpose - (Identify) - Documentation & training materials for OSS developers on good secure coding practices
  - *OpenSSF Best Practices Badge* (formerly CII Best Practices badge)
    - https://bestpractices.coreinfrastructure.org/ and https://github.com/coreinfrastructure/best-practices-badge
    - Purpose - (Identify/Adopt) Identifies FLOSS best practices & implements a badging system for those practices
  - *Scorecards Project*
    - https://github.com/ossf/scorecard
    - Purpose - (Adopt) Automate analysis and trust decisions on the security posture of open source projects
  - *Secure Software Development Fundamentals* (edX course)
    - https://openssf.org/training/courses/
    - Purpose - (Learn) Teach software developers fundamentals of developing secure software
  - *SKF - Security Knowledge Framework*
    - https://www.securityknowledgeframework.org/
    - Purpose - (Identify/Adopt/Learn) Learn to integrate security by design in your web application

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Recent Achievements (yay!)

- *Great MFA Distribution Project*
  - https://github.com/ossf/great-mfa-project
  - Distribute MFA tokens to OSS developers and best practices on how to easily use them

At the end of 2021, the WG helped distribute 102 Yubikey and 65 Titan keys donated by GitHub and Google to help OSS maintainers protect their identities using 2FA!

Security Knowledge Framework

- SKF now up to over 70 developer labs for nodejs, python, & java
- Working with the npm security team on npm security best practice guide
- Scorecards v4 launched in early Feb

Next Projects

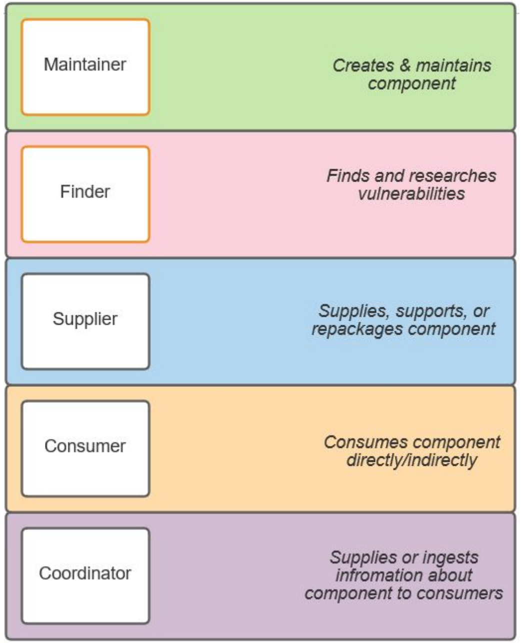
Upcoming Projects

- Recommended compiler option flags for C/C++ programs (incubating)
  - Recommended compiler option flags for C/C++ programs, especially warning and hardening flags, for developers & distributions
- *“Newbies View” Interactive artwork* - (incubating)
  - https://github.com/blabla1337/wg-best-practices-os-developers/tree/main/infinity2
  - Place where we want to guide developers in what stage they can use what type of tooling or approach. We have tons of great tools and materials but hard to find for devs, using this page and interactive loop we want to guide them to find the right stuff.
- *Package Manager Best Practices* - (incubating)
  - https://github.com/ossf/package-manager-best-practices
  - Purpose - (Identify/Learn) Collect and document security best practices for projects using various package managers.
- SECOM Convention - How to write a good security commit message
  - https://drive.google.com/file/d/1_UFPRDD9jvmlARxWshSu9WNV1ib_kCid/view

Vulnerability Disclosure

Update on Vulnerability Disclosure

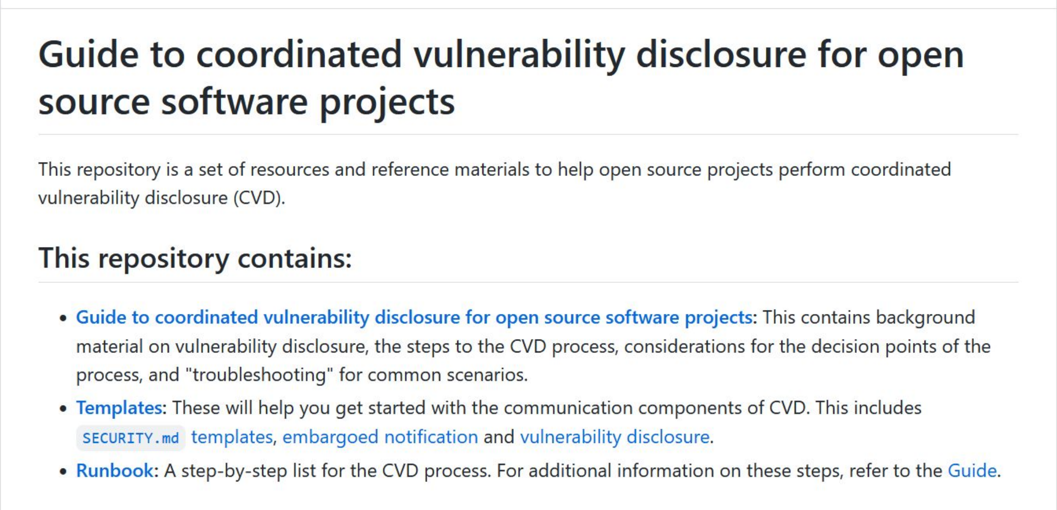
- Est. 26Feb2020
- ~ 25 Members, 10 very active
- Primary projects:
    - Guide to Coordinated Vulnerability Disclosure for Open Source Projects
    - Recommendations for Open Source Software Vulnerability Disclosure whitepaper (incubating)
    - OSS Vulnerability Disclosure Personas and Painpoints



Maintainer	*Creates & maintains component*
Finder	*Finds and researches vulnerabilities*
Supplier	*Supplies, supports, or repackages component*
Consumer	*Consumes component directly/indirectly*
Coordinator	*Supplies or ingests infromation about component to consumers*

Recent Achievements (yay!)

- Meetings with CVD Board to discuss open source CVS concerns and requirements and learn about changes to the program
- Publication of Guide to Coordinated Vulnerability Disclosure for Open Source Projects



Guide to coordinated vulnerability disclosure for open source software projects

This repository is a set of resources and reference materials to help open source projects perform coordinated vulnerability disclosure (CVD).

This repository contains:

- Guide to coordinated vulnerability disclosure for open source software projects: This contains background material on vulnerability disclosure, the steps to the CVD process, considerations for the decision points of the process, and "troubleshooting" for common scenarios.
- Templates: These will help you get started with the communication components of CVD. This includes `SECURITY.md` templates, embargoed notification and vulnerability disclosure.
- Runbook: A step-by-step list for the CVD process. For additional information on these steps, refer to the Guide.

Next Projects

- CVD Disclosure Guide for Security Researchers (aka Finders) engaging with OSS
- Meeting with CERT/CC to talk about open sourcing VINCE CVD tool
- FOSS Backstage panel on Zero Days & OSS CVD
- Maintainer Survey to learn how WG can assist OSS projects
- Collaboration with Omega project
- Vulnerability report formats

Securing Critical Projects

Update on Securing Critical Projects

- An initial short-list of “The most critical open-source projects”.
    - The main objective was to help inform Project Alpha-Omega and the Great MFA Project.
        - Great MFA Project - set a goal to complete in 2 weeks.
            - Wasn’t meant to be comprehensive due to time constraints
            - Initial output to help Great MFA project reps
        - Project Alpha - Help inform decision-making.
            - Completed a (rough) initial short-list of 100 Critical Projects.
    - Intended to be iterative, both qualitative and quantitative, and community-driven.
    - Completed first draft in time (thanks to workgroup coming together!)
- Since January, refining the process for a more comprehensive and representative list of the Most Critical Projects.
        - Develop further to prioritize and rank projects.
        - Iterate and improve process.
        - Awaiting release of full Census II project results (significant amounts of data) to analyze with workgroup.

Update on Securing Critical Projects

- Securing critical projects
  - Open Source Technology Improvement Fund
    - Facilitated a security review of the Flux Project (funded by CNCF), resulting in 22 security improvements, including the reporting and patching of the project’s first CVE.
    - Actively facilitating 15 security engagements for critical oss projects.
  - Allstar security policy bot
    - Installed on and scanned 20,400 unique repos in 422 organizations
    - Enabled on 2,000 unique repos in 101 organizations
- Miscellaneous updates:
  - Updated Github Page with refined goals: https://github.com/ossf/wg-securing-critical-projects/pull/33/files
    - 1. Identify critical open source software (OSS) projects.
    - 2. Secure those projects.

Identifying Security Threats

Update on Identifying Security Threats

- Security Insights (Lead: Luigi Gubello)
  - Share machine-readable security information that is hard/impossible to collect automatically.
  - Goal: Use as an additional data source for Scorecards, etc.
  - Examples: Project lifecycle, contribution policy, external distribution points, threat modeling, tools that aren't obvious in the repository.
- Security Reviews (Lead: Amir Montazery)
  - Public security reviews against open source projects (dashboard)
  - Over 35 reviews and counting.
- Security Metrics (Lead: Michael Scovetta)
  - Aggregates metrics from various sources (Scorecard, Criticality Score, Best Practices Badge, etc.)
  - Ongoing conversations around deprecation, likely to be replaced by LFX Security.
- Alpha-Omega
  - Will likely detach from this working group in the near future…

Alpha-Omega Project

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Mission

Protect society by improving the security of open source software through direct maintainer engagement and expert analysis

Update on Alpha-Omega Project

- Launched on Feb 1, 2022
- Seed funding provided by Google and Microsoft
- Leads: Michael Scovetta (Microsoft), Michael Winser (Google), Brian Behlendorf (LF/OpenSSF)

- In progress
  - Hiring full-time roles (product manager, security engineer, security analyst/researcher)
  - Governance and related
  - Initial Alpha engagements
  - Initial Omega toolchain, analysis, workflow

- Learn More
  - Read the press release, watch the webinar, join the #alpha_omega slack.
  - Join the announcement mailing list.

Q&A

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Get Involved

- Join a Technical Working Group - https://github.com/ossf
- Join the Mailing List - subscribe to the openssf-announcements mailing list
- Join our Public Meetings - https://bit.ly/ossf-calendar
- Join our Slack Channel - https://slack.openssf.org
- Watch YouTube Channel - https://bit.ly/ossf-youtube
- Feedback?
    - Drop us an email! - operations@openssf.org

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Thank You!