# OpenSSF WG/Alpha-Omega Monthly Sync

## Meeting Notes

### 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.

## Planned Meetings

Meetings take place monthly, scheduled on the OpenSSF Community Calendar. (Look for a meeting titled “Alpha-Omega Project Public Meeting”.)

# 2025-09-03 Meeting

Attendance

- Munawar Hafiz (OpenRefactory)
- Salve J. Nilsen (CPANSec)
-

Topics

- Overview of KERI (keri.foundation) from Samuel Smith

# 2024-02-07 Meeting

Attendance

- Michael Scovetta (Alpha-Omega, Microsoft)
- Seth Larson (PSF)
- Jonathan Leitschuh
- Sally Cooper (Linux Foundation Marketing)

Topics:

-

# 2024-01-03 Meeting

Attendance

- Seth Larson (PSF)
- Michael Scovetta (Alpha-Omega, Microsoft)
- Ataf Ahamed (OpenRefactory)
- Fatima Alam
- Jonathan Leitschuh
- Jeffrey Borek (IBM)
- Michael Winser (A-O)
- David A. Wheeler
- Andres Orbe

Topics:

- "A-O as a grant-making organization"
- What about Omega?

    - AI
    - Shoveling sand on the beach
    - "Ecosystem Safety Engineer"
- Mobb.ai: ChatGPT in Vulnerability Remediation Comparative Analysis: https://mobb.ai/blog/chatgpt-in-vulnerability-remediation-a-comparative-analysis
- In Need of 'Pair' Review: Vulnerable Code Contributions by GitHub Copilot (Black Hat): https://www.youtube.com/watch?v=xz-zs7GRQ7U
- https://aicyberchallenge.com
- AI/ML & Security slides: https://dwheeler.com/secure-class/presentations/AI-ML-Security.ppt
- https://youtu.be/xz-zs7GRQ7U?si=Dt56VmFbeqO_QUKn
- If you take away availability, we solved security. But security includes availability.
- AIxCC: https://aicyberchallenge.com/
- For background on OpenSSF/AIxCC connection see: https://openssf.org/press-release/2023/08/09/openssf-to-support-darpa-on-new-ai-cyber-challenge-aixcc/
- David A .Wheeler: AI/ML & Security slides: https://dwheeler.com/secure-class/presentations/AI-ML-Security.ppt ; older version of this as a video is here: https://www.youtube.com/watch?v=kTMgG5gn-oU#t=10m52s
- https://www.cisa.gov/securebydesign
- Secure By Design Paper:
    - Older April 2023 version: https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
    - October 2023 version: https://www.cisa.gov/resources-tools/resources/secure-by-design
    - Review/commentary by David A. Wheeler: https://openssf.org/blog/2023/10/23/secure-by-design-guidance-from-governments/
- Currently CVE process doesn't consider "Insecure by default" as a vulnerability. E.g., every JavaScript XML parser is vulnerable, because "insecure by default" isn't considered a vulnerability.
    - David A. Wheeler will pitch to the CWE folks about adding "Insecure by Default" as a vulnerability class. Then it'll be much easier to convince the CVE process to allocate CVEs to those vulnerabilities
-

# 2023-12-06 Meeting

Attendance

- Zach Steindler (GitHub, OpenSSF TAC)

- Seth Larson (PSF)
- Michael Scovetta (Alpha-Omega, Microsoft)
- Ataf Ahamed (OpenRefactory)
- Amir Montazery (OSTIF)
- Nick Vidal (ClealyDefined, Open Source Initiative)
- Brian Crooks (Datalytica)

Topics:

- [ZS] Budget / funding cycle / application process
    - Always room for consideration! Applications are considered on a rolling process (we're working on responding to applications more quickly)
    - Moving to a quarterly model
        - First month: solicit ideas
        - Second month: refine ideas / proposals
        - Third month: fund!
        - … repeat so you don't feel like you've "missed the train"
        - … but also not yet at quarterly model
    - https://alpha-omega.dev/grants/how-to-apply/
        - First, then Michael Winser will reach out
- [MW] A-O Portfolio model
    - First investment category: staffing security-oriented team at an existing mature organization
        - These are few and far between, and can be expensive
    - Second category: "app stores of open source" e.g. package repositories (PyPI, Homebrew)
        - Huge downstream benefits to users of these package / language ecosystems
    - Third category: things that can be packaged as a project with a beginning, middle, and end, like an audit
        - Things that don't have ongoing maintenance
    - Fourth: everything else! Trials, experiments
    - These categories are roughly ordered to reflect scale of investment
- [MW] What makes a good application?
    - Looking for impact, and on a clear timeline with immediacy
        - Broad or deep - doesn't matter
    - Shovel-ready bias, not research that might be applied years from now
    - Projects should give early feedback back to A-O so we can iterate and change course
    - Alpha is single points with high impact - large ecosystems, lots of users
    - Omega is about frameworks / patterns that are widely applicable to lots of projects
- [MS] Thoughts on "bending the curve" on the long tail
    - What sort of things can we do that positively impact lots of projects at the same time?

    - SL: There's a Python ecosystem contributor, Hugo, who does tooling-assisted fixes across many projects when there's a vulnerability, or backwards incompatibility issue
        - Having these fixes come from an entity that's known in the ecosystem is huge - a person with a reputation instead of an anonymous bot
        - MW: interested in how we "invert the cost" of security work. "Keep updating to main" is a treadmill some people are tiring of. "Changer pays" means you can add system-wide security capabilities, if you have the tooling to update all the places.
    - HY: where does all the compute come from to see if tests pass with a proposed change?
        - MS: today CI run results are available to project maintainers, but not necessarily someone who's coming in and proposing the change (preventing "changer pays")
    - When we deprecate a function, can we provide a machine-understandable way how to replace calling the old function with calling a new function?
        - Is there a way to provide a "heat-map" about what functions are being called?
        - Could do static analysis of public code - telemetry of private usage is probably off the table
    - A mind-shift in testing - instead of testing the code your write, also testing the code that you depend on. Would it be possible to generate this testing automatically?
    - Maven provided plugins automatically to easily drive ecosystem adoption
    - Scaling operations of malware detection on PyPI by taking a manual process that humans respond to, and turning that into an API that partners can integrate with.
    - There's a disincentive to pre-release software… because nobody uses the pre-release! Could we make it easier for people to test / evaluate pre-releases?
    - Could there be a signaling mechanism between organizations and projects?
        - Not necessarily for blocking (except in actual cases of malice), but annotating (this version of log4j has known vulns, but maybe there is a reason you'd like to use it)

# 2023-11-01 Meeting

Attendance

- Michael Scovetta (Microsoft / Alpha-Omega)
- Ataf Fazledin Ahamed (OpenRefactory)
- Zach Steindler (GitHub, OpenSSF TAC)
- Munawar Hafiz (OpenRefactory)
- Amanda Martin (Linux Foundation)
- Seth Larson (PSF)

Topics:

- https://github.com/ossf/alpha-omega/blob/main/alpha/engagements/2023/psf/update-2023-10.md
- https://github.com/ossf/alpha-omega/blob/main/alpha/engagements/2023/OpenRefactory/update-2023-10.md
- https://openjsf.org/announcement/2023/11/01/openjs-foundation-warns-consumer-privacy-and-security-at-risk-in-three-quarters-of-a-billion-websites/
- How do we manage the spectrum of early projects to critical projects?
    - Things like https://github.com/ossf/security-insights-spec make the intent much more explicit
    - … but of course intents aren't always reality

# 2023-09-06 Meeting

Attendance (please add yourself):

- Michael Scovetta (Microsoft / Alpha-Omega)
- Seth Larson (PSF)
- Munawar Hafiz (OpenRefactory)
- Yesenia Yser (LF, Alpha-Omega)
- Ataf Fazledin Ahamed (OpenRefactory)

# 2023-07-05 Meeting

Attendance (please add yourself):

- Michael Scovetta (Microsoft / Alpha-Omega)
- Seth Larson (PSF)
- David Edelsohn (IBM, CTI)
- Glenda Garcia (LF, Alpha-Omega)
- Aaron Blume (LF, Alpha-Omega)
-

Topics:

- Updates from Alpha-Omega

# 2023-06-07 Meeting

Attendance (please add yourself):

- Michael Scovetta (Microsoft / Alpha-Omega)
- Munawar Hafiz (OpenRefactory)

- Annapurna V (Citi / Alpha-Omega)
- Ben Edgar
- Yesenia Yser (LF, Alpha-Omega)
- Andres Orbe (LF, Alpha-Omega)
- Glenda Garcia (LF, Alpha-Omega)
- Aaron Blume (LF, Alpha-Omega)
- *Please add yourself*

Topics:

- Updates from Alpha-Omega
- Updates from NodeJS
    - Permission model -> collecting feedback. Security feature to deny access on resources (worker threads, internals)
- Invite Alpha engagement resources to join and provide their updates on this meeting from next week.
- Alpha-Omega Website went live!
    - https://alpha-omega.dev
- https://github.com/ossf/disclosure-check
- Mentorship Program Updates from YY & JL
    - Omega Engineering Software Requirement Document
        - Goal is to provide connectivity between the analyzer and the triage portal for local or cadence scan build model
    - Mentee Introduction
- OpenSSF Day A-O Talk: https://www.youtube.com/watch?v=vNqA5Qo0nnE
- Updates from OpenRefactory (Munawar): https://github.com/OpenRefactory-Inc/oss-bug-fixing-campaigns
-

# 2023-05-03 Meeting

Attendance (please add yourself):

- Michael Scovetta (Microsoft / Alpha-Omega)
- David Edelsohn (IBM, CTI)
- Munawar Hafiz (OpenRefactory)
- Noah Spahn (The Open University)
- Randall T. Vasquez (LF/Gentoo)
- Yesenia Yser (LF, Alpha-Omega)
- Veena Ambalavanan
- *Please add yourself*

Topics:

- Certification for "Security Researcher" - the name is too broad
    - "Smashing the Web"

    - Tie into sos.dev?
    - Other existing content?
    - Cred.ly
    - Go through LF?
    - Badges in Github -> part of mobilization plan
    - Future idea -> certification and/or badge needed for access to Triage portal (future prod)
- Reporting vulnerabilities privately
    - PoC: https://github.com/scovetta/disclosure-check
    - Come discuss on #wg_vulnerability_disclosures_autofix
    - OpenSSF CERT (CRob)? - currently with OpenSSF/GB.
        - https://github.com/ossf/SIRT/tree/main/plan
        - https://github.com/ossf/SIRT/blob/main/plan/initial_discovery.md
- Omega Triage Portal - Should be available shortly (publicly), but you can run it yourself today.
- Open Q&A

# 2023-04-05 Meeting

Attendance (please add yourself):

- Munawar Hafiz (OpenRefactory)
- Yesenia Yser (LF, Alpha-Omega)
- David A. Wheeler (Linux Foundation)
- Randall T. Vasquez (SKF/Gentoo)
- Ben Edgar

Topics:

- Proposal from ISRG
- April 10 - Paid mentorship program through the linux foundation mentorship portal
    - Will say ‘Application Closed’ until April 10
    - LF Mentorship Program: https://mentorship.lfx.linuxfoundation.org/#projects_all
    - Application: https://mentorship.lfx.linuxfoundation.org/project/4df8fab8-e11a-4877-8140-c3633099ea24
- Welcome feedback, pull request, and issues for Assurance Assertions Framework
    - https://bit.ly/assuranceassertions
    - ossf/Alpha-Omega in Github
- Open Source In NA / OpenSSF Day Talks
    - https://ossna2023.sched.com/event/1K5Ay/scaling-the-security-researcher-to-eliminate-oss-vulnerabilities-once-and-for-all-jonathan-leitschuh-open-source-security-foundationlinux-foundation - Jonathan talks about finding oss vulns at scale

    - https://openssfna2023.sched.com/event/1KriY?iframe=no Alpha-Omega Panel with Munaware, Ram Iyengar, Mikaël Barbero, Walter Pearce, and Yesenia Moderating

# 2023-03-01 Meeting

Attendance (please add yourself):

- David A. Wheeler (Linux Foundation)
- Yesenia Yser (Linux Foundation, Alpha-Omega)
- Munawar Hafiz (OpenRefactory)
- Jonathan Leitschuh (Linux Foundation, Alpha-Omega)
- Sebastian Crane
- Amir
- Nick Vidal (Open Source Initiative, ClearlyDefined)
- Randall T. Vasquez (SKF, Gentoo)

Topics:

- Are there any questions from the public?
- There's been a subtle adjustment as we examine Omega further - automated patch creation.
    - Many security researchers find specific vulnerabilities in a specific program, but there are some vulnerabilities that cross across a large number of programs, where you can create a pattern that creates a pull/merge request for a large number of OSS projects.
    - This is something we can uniquely do - if 300 programs have the same mistake, instead of having 300 developers create the fix 300 times, create automated proposals for each that fix it everywhere.
    - Jonatha Leitschuh is uniquely expert in doing this, so we hired him, he's working on preparing new ones, as well as creating policies & getting them discussed.
    - Some developers are concerned that these automated proposals will overwhelm them, as if they're spam. We think we can address those concerns.
- Some things tackled
    - Zipslip. Is it vulnerable & then fix it.
    - Openrewrite - preserves the formatting. Also see Moderne.
    - Still working on the process for how the PRs will be created.
    - Jonathan has run these campaigns before.
    - David: Do in stages, review earlier proposed changes by hand before release, once we have a lot of confidence start increasing, put other things in place to prevent spamming, do rate limiting to prevent an error becoming a widespread problem.
- How about a self-service to ask to be added?
    - E.g., an explicit opt-in into this program.

    - Jonathan: I often run the scripts at scale, looking at the results, then triage. Hadn't considered opt-in early, but that could be done.
    - David: One term is "phased roll-out". We basically don't want to send out all changes at once, even though we want to know them internally (so we can have confidence that it's correct). Could allow project to opt in to be part of the first phase of a phased roll-out.
- Not all projects on GitHub enable private vulnerability disclosure
    - GitHub has recently added private vulnerability reporting: https://docs.github.com/en/code-security/security-advisories/guidance-on-reporting-and-writing/privately-reporting-a-security-vulnerability
    - However it's in beta & off by default
    - We could ask the projects to turn in on weeks when we realize we have something to report, they don't have it on, and we haven't contacted them before. Then say we'll file publicly in 2 weeks
- Big difference between detecting *one* vulnerability & sharing that across many projects
    - There are many great tools that do deep dives to find vulnerabilities in specific programs for specific situations.
    - Some of those, however, are examples of a widespread pattern. Once we determining a pattern, we can use different tools to detect the code pattern; they need some similar capabilities (e.g., data flow is helpful), but it's a different kind of analysis.
-

# 2023-01-04 Meeting

Attendance (please add yourself):

- Michael Scovetta (Microsoft, Alpha-Omega)
- Michael Winser (Google, Alpha-Omega)
- David A. Wheeler (Linux Foundation)
- Yesenia Yser (Linux Foundation, Alpha-Omega)
- Rosaria Carr (Indeed)
- Munawar Hafiz (OpenRefactory)
- Jonathan Leitschuh (Linux Foundation, Alpha-Omega)
- Randall T. Vásquez (SKF, Gentoo)
- Marta Rybczynska, Syslinbit
- Fridolin Pokorny (Datadog)

Topics:

- Project Updates
- One of Jonathan's talks (SEC-T 0x0E): https://www.youtube.com/watch?v=WkdzWiNKzt8

- Leveraging universities for security fixes
    - Munawar to connect with Yesenia about this project.
- Incentives for security work in open source:
    - Sos.dev
    - Internet bug bounty
    - SKF (bug bounty platform?)
    - Per-org security sponsorships
    - Alpha-omega

# 2022-12-07 Meeting

Attendance (please add yourself):

- Michael Scovetta (Microsoft, Alpha-Omega)
- Joshua Lock (VMware)
- Jon Zeolla (Seiso)
- Sal Kimmich (EscherCloud)
- Yesenia Yser (Linux Foundation, Alpha-Omega)
- Rosaria Carr (Indeed)
- Munawar Hafiz (OpenRefactory)
- Fridolin Pokorny (Datadog)

Topics:

- Project Updates
- Assurance Assertions
- Joshua Lock: Yocto Project & Alpha-Omega
- Sal Kimmich: Maintainer Training/Ecosystem Hardening
- Munawar: Expanding the PyPI scan, triage, fix project
- Need to have a conversation around GitHub expanding out private security issues (opt-in vs. opt-out).
- Issue -> sos.dev

# 2022-11-02 Meeting

Attendance (please add yourself):

- Eric Tice (Wipro)
- Michael Scovetta (Microsoft, Alpha-Omega)
- Michael Winser (Google / Alpha-Omega)
- Randall T. Vasquez (Gentoo)
- Frank Yen
- Andrew Aitken
- Rafael Gonzaga (Nearform)
- David A. Wheeler (Linux Foundation)
- Arathi Nair

- Aaron Wislang (Microsoft)
- Munawar Hafiz (OpenRefactory)
- Georg Kunz (Ericsson)
- Renuka Kularni

Topics:

- Welcome
- Update from Node.js (Rafael Gonzaga)
    - Added threat model (recent pull request) - some things aren't considered a threat on node.js, for example. Created by security WG.
    - See "Node.js Security WG Collab" slides (briefly presented):
      Node.js Security WG - Collab Summit
        - Issue: What about when vulnerabilities are discovered in our dependencies (direct & indirect)? E.g., OpenSSL?
            - GitHub actions notify node.js about them.
            - Q: Is this just using something out-of-the-box from GH? Is something reusable by other projects?
        - Q: Is Node.js plumbed into the embargo process for OpenSSL (and others)? [When did Node.js learn about the OpenSSL vulnerability?]
            - Node actually uses QuicTLS (fork of OpenSSL)
        - Threat model - many security researcher reports (35%) are closed N/A, making it clear that many security researchers don't understand the threat model on node.js
            - David: There are some terminology differences. Some call this kind of information "security requirements" & others "threat model" - but whatever you call it, it's important to know what it's supposed to do & not do.
        - Q&A:
            - It's REALLY helpful to know that a vulnerability WILL be announced on a particular day. They have a 42-step process to release a security release, it takes about a week, knowing it will happen is really helpful. (Example: OpenSSL). It might be good to tell the vulnerability disclosures working group.
            - They don't currently use VEX to report when a vulnerable dependency doesn't affect Node.js, that has been discussed.
    - Added best practices
- Michael: (per open issue) Attestation/assertions: https://github.com/ossf/alpha-omega/issues/28
    - David: I think it'd be useful, at least to say "Tool X found no vulnerabilities [at critical/high level] in software version XYZ". Don't say if you DID find issues; false positives are pretty common & there's little point in helping attackers by doing part of their work for them.

        - “This feels like a "no failing tests" when you're picking up a new repo.” - Aaron Wislang. That is, it’s not a guarantee, but it’s a useful signal to recipients.
    - How can others confirm?
        - Use digital signatures. Sigstore signatures are much easier to verify & are recorded in a transparency log, consider using that.
        - We can make sure the process can be duplicated.
- Docker container of tools: Please do comment, send feedback.
    - It should be easy to rebuild. Let us know if there are features you’d really like.
    - It’s intended for security researchers, not for organizations to examine their own repo, though we imagine it could be used that way.
    - Java ecosystem support is weak, needs improvement.
    - .NET - same thing, doesn’t do a lot with compiled code.
    - Many tools want source code - doesn’t do a lot with compiled versions.
    - David: Ideally would be able to give a compiled package, automatically get its source code, and analyze it all.
- What about selecting critical projects?
    - OpenSSF Critical Projects WG has been working to ID critical projects based on quantitative analyses (Census I, Census II, criticality score) & human knowledge
    - Different verticals (e.g., FINOS) will almost certainly have a different list. Critical Projects WG has discussed providing not just a list, but a “franchisable/reusable” process that verticals can re-apply.
- Some of us can’t use Slack
    - No problem! Just use the mailing list, most organizations allow that.

# 2022-10-05 Meeting

Attendance (please add yourself):

- Eric Tice (Wipro)
- VM Brasseur (Wipro)
- Michael Scovetta (Microsoft, Alpha-Omega)
- Michael Winser (Google / Alpha-Omega)
- David A. Wheeler (Linux Foundation)
- Randall T. Vasquez (Gentoo)
- Varun Sharma (StepSecurity)
- Warren Grunbok (IBM)
- Munawar Hafiz (OpenRefactory)

Topics:

- Welcome

- Discussion on the Core Infrastructure Initiative – are there things we can learn from that experience?
- Action: Invite maintainers for popular Linux distros to the virtual summit. https://openssf.slack.com/archives/C040JBS9S59
    - https://docs.google.com/presentation/d/1xjY2jkYBsFwWpLgICEV6HpBiUtoclSBGBD7sL-RrMXA/edit?disco=AAAAhaNnu0I
    - https://docs.google.com/presentation/d/1xjY2jkYBsFwWpLgICEV6HpBiUtoclSBGBD7sL-RrMXA/edit?disco=AAAAhaNnu0M
-

# 2022-09-07 Meeting

Attendance (please add yourself):

- Michael Scovetta (Alpha-Omega/Microsoft)
- Eric Tice (Wipro)
- VM Brasseur (Wipro)
- Rafael Gonzaga (Alpha-Omega/Nearform)
- Randall T. Vasquez (Gentoo)
- Munawar Hafiz (OpenRefactory)

Topics:

- Welcome
- Short Deck
    - Node.js updates (including new permission model)
        - https://github.com/ossf/alpha-omega/tree/main/alpha/engagements/2022/node.js
    - Omega Tracer: https://github.com/scovetta/omega-stracedb
- Open Discussion (most of our time be just here)
    - Actions:
        - A-O to talk/think about verticals and how we can/should engage, at least for exploratory conversations. – e.g. automotive, healthcare, financial, etc. – build trust, etc.
        - A-O to talk to to a few organizations:
            - Randall to start conversation here with Mike (Homebrew) and Sam (Gentoo)
    - Risk Scoring? -> (Criticality Score * Scorecard * Dependency Graph * Existing CVEs * Omega Findings)
        - Predictive model? Something for academics to tackle?
    - Possibility: “Project of the Month” -> sos.dev?
    -

# 2022-07-20 Meeting

Attendance (please add yourself):

- Michael Scovetta (Alpha-Omega/Microsoft)
- Eric Tice (Wipro)
- VM Brasseur (Wipro)
- Munawar Hafiz (OpenRefactory)
- Brian Behlendorf (OpenSSF / LF)
- Rafael Gonzaga (Alpha-Omega/Nearform)
- David Edelsohn (IBM, GCC)

Topics:

- Short Deck
- Add topics here, or just start talking. :-)

# 2022-06-01 Meeting

Attendance (please add yourself):

- Michael Scovetta (Alpha-Omega/Microsoft)
- Michael Winser (Alpha-Omega/Google)
- Jeff Borek (IBM)
- Morten Linderud (Arch Linux)
- Jonathan Leitschuh (Dan Kaminsky Fellowship @ HUMAN Security)
- Georg Kunz (Ericsson)
- Amir Montazery (ostif)
- Khahil White (Linux Foundation)
- Jory Burson (Linux Foundation)
- Vinod Anandan (Citi)

Agenda

-

# 2022-05-06 Meeting

Attendance (please add yourself):

- Michael Scovetta (Alpha-Omega/Microsoft)
- Andrey Khalyavin
- Michael Winser (Alpha-Omega/Google)
- David A. Wheeler (Linux Foundation)
- Jory Burson (Linux Foundation)
- Wietse Z Venema (Google)

- John Naulty (Coinbase)
- Eric Tice (Wipro)
- Jordan Harband (Coinbase)
- Jeff Borek (IBM)

Agenda

- Welcome / Introductions
    - Hi new Friends!
- Hiring
    - Still open, send folks to the job descriptions to apply.
        - https://openssf.org/community/alpha-omega/
- Alpha
    - Node.js announced as first Alpha engagement: https://openssf.org/blog/2022/04/18/openssf-selects-node-js-as-initial-project-to-improve-supply-chain-security/
        - First Meeting with Node stakeholders rescheduled for next week (May 11)
        - Action: Invite Node TSC representative to monthly Alpha Omega call
- Omega
    - Automated reviews: PoC / testing
        - PR open, feedback welcome: https://github.com/ossf/security-reviews/pull/73
- Other Topics
    - Data that would be interesting to gather from A-O project?
        - Examples/Cases of using X tools well
        - # Vulns found and fixed
        - Coverage in the npm ecosystem
        - “# of Jordan Harbands helped”
            - How many Jordans are there? People who have X%

# 2022-04-06 Meeting

Attendance (please add yourself):

- Michael Scovetta (Alpha-Omega/Microsoft)
- David A. Wheeler (Linux Foundation)
- VM Brasseur (Wipro)
- Andrew Aitken (Wipro)
- Brian Behlendorf (LF)
- Jenn Bonner (LF)
- Jory! (Burson) (LF)
- Bhavneet Chugh
- Jonathan Leitschuh
- Alex KIm(IBM)
- Jacques Chester (Shopify)

- Altaz Valani (Security Compass)
- Jack Aboutboul (AlmaLinux)
- Eric Tice (Wipro)
- Christine Abernathy (F5)
-

Agenda

- Remember to Record
- Welcome / Introductions
- Job postings
    - Jobs have been posted!
    - 7 phone screens in hopper
    - Current plan is to fill the PM role first if we can
    - We're trying to reach out to other locations, esp. for traditionally underrepresented.
    - Please *DO* point people to the job postings!!
    - See: https://openssf.org/community/alpha-omega/
    - Anyone have other good job boards to post to? Let us know (email Jory)
- We have an initial Alpha project, not quite ready to announce yet (still working on things for the announcement), it's an important project in need of help
    - In the longer term we want to cover multiple language ecosystems
    - Want to work on capacity building
    - Will have a 9 month engagement, engaging 2 organizations to help, we'll have monthly oversight. Key part: Take vulnerability reports & turn into actionable results, helping them handle reports more efficiently. Assist with triage pipeline and security posture training for existing maintainers.
    - It'll be a combination of addressing known vulnerabilities & improving processes overall.
- Q&A
    - VM: Is this call monthly? Or different frequency?
        - We scheduled it monthly. If the time is bad, we can move it to a different time. Anyone can join this meeting, don't need to be an OpenSSF member
        - "This is like open office hours" - enables anyone to visit, ask questions, have discussions.
    - Only short time to WH executive meeting, e.g., Moonshot. Does that affect anything?
        - Michael Scovetta: I don't have more info.
        - Finding more resources for alpha-omega is something we want to see, currently want others to join at same level. That'll be easier to argue once we've had some successes, so we're working on having some successes.
        - Alpha-Omega isn't dependent on government grants, we haven't applied for any of them. (It could be done but it's not currently our focus.) We aren't going to do government lobbying.

        - David W: Alpha-Omega was conceived before the WH meeting. We just want to move forward, & the more we can work with others long-term that's great… but we don't want to wait for that. Let's make progress & then others can join / work with us as they choose.
        - Brian: A lot of governments are just looking into establishing OSPOs, which seems like table stakes compared to industry practice (industry has been doing this for years).
        - We've reached out to Aspen Group, Atlantic Council, Plaintext Group, openUK.
    - Does Alpha-Omega Project have part-time positions for the Lead PM just to get started with the basics?
        - David W: The lead PM is advertised as a full-time position.
        - For part-time, best thing to do is to get involved in the OpenSSF WGs, because alpha-omega will build on their work
    - Should we extend this meeting from ½ an hour?
        - We can expand to an hour. At least for now monthly seems sensible.
    - How should Omega handle bug bounty payouts (does the researcher get it? Split it? Give it to charity? Give it back to Alpha-Omega? Something else?
    - Note: If you want to discuss things Alpha-Omega at other times, feel free to join the endless party / endless rave of its Slack channel :-)