Alpha-Omega

2022 Annual Report

DECEMBER 2022

Michael Scovetta (michael.scovetta@microsoft.com)
Michael Winser (michaelwinser@google.com)

Contents

What is Alpha-Omega?

Alpha-Omega is an OpenSSF project with a mission to protect society by improving the security of open source software through direct maintainer engagement and expert analysis. It was established in February 2022 with a $5 million grant made jointly by Google and Microsoft, with a vision that critical open source projects are secure and that security vulnerabilities are found and fixed quickly.

Through the "Alpha" side of Alpha-Omega, we identify parts of the open source ecosystem where funding security work could have broad and exceptionally high impact. To date, our investments here have been largely focused on improving the security of core platforms and programming languages, as well as foundations that represent a significant number of critical projects.

Through the "Omega" side of Alpha-Omega, we use high-quality security tools and expert analysis to identify critical vulnerabilities at scale, across the 10,000 most-critical open source projects, and collaborate with maintainers to get those vulnerabilities fixed.

The Alpha-Omega Project values experimentation. While the best way to address security risk within the open source community isn't clear-cut, we'll make investments, learn what works and what doesn't, and refine our approach over time. We welcome community input on the methodologies used to select projects and the types of activities that will have the greatest impact.

Sponsors and Supporters

We would like to thank the following organizations for sponsoring the Alpha-Omega project. With their financial assistance, improving the security of open source software has been made possible.

Engagement Partners

We'd also like to thank our partner organizations associated with our Alpha engagements; these organizations maintain software used by millions of developers and billions of end-users.

Highlights from Our First Year

Notable highlights from the Alpha-Omega project's first year include funding important security work across four different ecosystems, including Node.js, the Eclipse Foundation, the Python Software Foundation, and the Rust Foundation. These engagements led directly to the following:

- The Node Security Working Group was reactivated and has started to create a threat model for Node.js. The team has been working on an experimental permissions model for Node modules, and are adding automated vulnerability checks to the Node.js continuous integration infrastructure. Finally, they've been able to triage over 20 vulnerability reports and issue multiple fixes, which directly improved the security of the Node.js runtime.
- The Eclipse team ran Security Scorecards against all Eclipse Foundation projects, analyzed the results, and created a prioritized list of activities that they'll focus on to achieve the best and broadest impact, which include hardening the build infrastructure and enabling security tools.
- We released an open-source analysis toolchain designed to target open source packages, and used this toolchain to identify multiple vulnerabilities in critical open source projects.

"Open source software security is a shared responsibility. Through our contribution, we're helping to fund the important work that Alpha Omega is doing across a broad range of open source communities. By combining efforts with others to find and fix vulnerabilities in critical open source projects, everyone who uses and builds on open source can also share in the benefits of a more secure software supply chain."

— DAVID NALLEY, HEAD OF OPEN SOURCE STRATEGY AND MARKETING, AMAZON WEB SERVICES

In addition, we've reached an agreement with Amazon Web Services to provide $2.5 million in funding to Alpha-Omega. Special thanks to David Nalley from Amazon Web Services for supporting us. We've also started to explore a partnership with the Financial Services Information Sharing and Analysis Center (FS-ISAC); special thanks to Jonathan Meadows from Citi/FS-ISAC, and Amanda Cody from FS-ISAC for helping to drive this forward.

"In today's financial services sector, software enables all our businesses. Understanding and securing the software supply chain is a critical element of our members' security programs. FS-ISAC is excited to partner with Open SSF's Alpha-Omega project and the open-source community to support our members' open source software risk management efforts."

— AMANDA CODY, CISO, FS-ISAC

How We Work

The Alpha-Omega project is managed by a core leadership team, including Michael Scovetta, Principal Security PM Manager at Microsoft and Michael Winser, Group Product Manager at Google, with support from the Linux Foundation (Brian Behlendorf, David A. Wheeler, Khahil White, Jenn Bonner, Jory Burson, Jennifer Bly, and Michelle Martineau) and Citi (Annapurna Veeramachaneni).

We're thrilled to announce that we've filled our first dedicated role on the Alpha-Omega team. Yesenia Yser will be focused on applying software engineering to solve our security challenges at scale. We've extended another offer and hope to have an additional announcement soon.

We hold public meetings once a month and maintain a public Slack channel within the OpenSSF Slack workspace. We provide regular updates to the OpenSSF Technical Advisory Council (TAC) and maintain close relationships with other OpenSSF working groups and projects.

Decisions are made collaboratively. To date, all significant decisions have been unanimous among the core leadership team.

Funding

In 2022, we raised a total of $6 million, with $2.5 million each coming from Google and Microsoft, and an additional $1 million coming from Google via the Secure Open Source Rewards program. With an average grant size of just under $350,000, these funds were used to provide over $2 million in direct funding to critical open source projects as shown in the table below.

Alpha Engagement	Date	Amount
Node.js	April 2022	$300,000
Rust Foundation	October 2022	$460,000
jQuery	October 2022	$350,000
Eclipse Foundation (Part 1)	October 2022	$400,000
Eclipse Foundation (Part 2)	November 2022	$150,000
Python Software Foundation	December 2022	$400,000
	Total:	$2,060,000

In 2023, we have a goal of raising $10 million from an increasingly broad set of organizations. We're confident that contributors, including Microsoft and Google are committed to remaining involved and contributing additional funds.

As mentioned earlier, we're proud to announce that we've received a commitment from Amazon Web Services to contribute $2.5 million to Alpha-Omega.

Outcomes

Alpha	**Engagements**	**6**
	Security Champions Hired	**3**
	Average Engagement Funding	**$343,333**
	Vulnerabilities Fixed	**20**
Omega	**Vulnerabilities Discovered**	**11**
	Vulnerabilities Fixed	**8**
Operational	**Conference Talks**	**2**
	Community Sessions	**6**
	Press Releases & Blog Posts	**6**
	Full-Time Staff	**1**
	Supporting Staff	**9**

For additional information, please see the reports that are provided as part of each Alpha engagement.

Drivers of Success

The Alpha-Omega project has had some key successes during its first year which we believe are due to a few guiding principles:

- **Clarity of Vision:** During the project's inception, we spent a lot of time talking about what we wanted to achieve, the ways that we would approach the problem space, the types of activities we would and wouldn't consider. Having a clear strategy allowed us to have those important conversations early, come to an agreement, and begin executing quickly.
- **Agency:** The Alpha-Omega core team is empowered to make the necessary decisions to drive the project forward, with periodic reporting back to their respective organizations and the OpenSSF TAC. We believe this allowed us to apply a bias for action, experiment, and provide funding in ways that would have been harder with a larger consensus pool.
- **Freedom to Experiment:** A core principle that we follow is that we should deliberately experiment. We accept that some of our investments will fail to deliver the results we hope for, but we expect to learn as much from those as the ones that are a resounding success.

Oversight & Alignment

Despite the success we've had in our first year, we recognize the need for checks and balances to ensure that we operate with the right level of oversight and alignment with OpenSSF broadly and transparency for the larger community. To that end, we commit to the following three activities:

BE EXPLICIT ABOUT AVOIDING SELF-DEALING

Alpha-Omega will avoid funding any open source project that is governed by any organization that funds Alpha-Omega. This means that we will not consider funding npm (because it's owned and governed by GitHub, which is owned by Microsoft), TensorFlow (owned and governed by Google), or FreeRTOS (owned and governed by Amazon). This approach only applies to monetary funders of Alpha-Omega, and not to OpenSSF as a whole or its members; for example, we might consider funding React despite it being maintained by Meta, as Meta does not currently provide funding to Alpha-Omega.

INCREASE OPENSSF TAC ENGAGEMENT

To ensure our plans align with the technical vision of the OpenSSF, we will be more deliberate in socializing funding plans to the OpenSSF TAC on a regular basis. This will allow members to raise strong objections or request clarifications. However, we will not be seeking formal approval from the TAC; allocation of Alpha-Omega funds are at the discretion of the Alpha-Omega core leadership team. Rather, it's an opportunity to "raise a flag" in case an allocation seems inappropriate on its face.

We will also increase the level of discussion we have with the OpenSSF TAC. We already meet periodically to brief the TAC on our progress and discuss relevant topics, but we'll expand this to include a deliberate, strategic discussion on the types of open source projects that Alpha-Omega should consider talking to.

INCREASE TRANSPARENCY ON FUNDING DECISIONS

Going forward, as part of our announcements, we will publish the rationale for investments, and in most cases, we'll include the engagement term sheet (activities and expected outcomes) within our **public GitHub repository**. We'll continue to hold monthly community meetings and be available on the public **#alpha_omega** Slack channel.

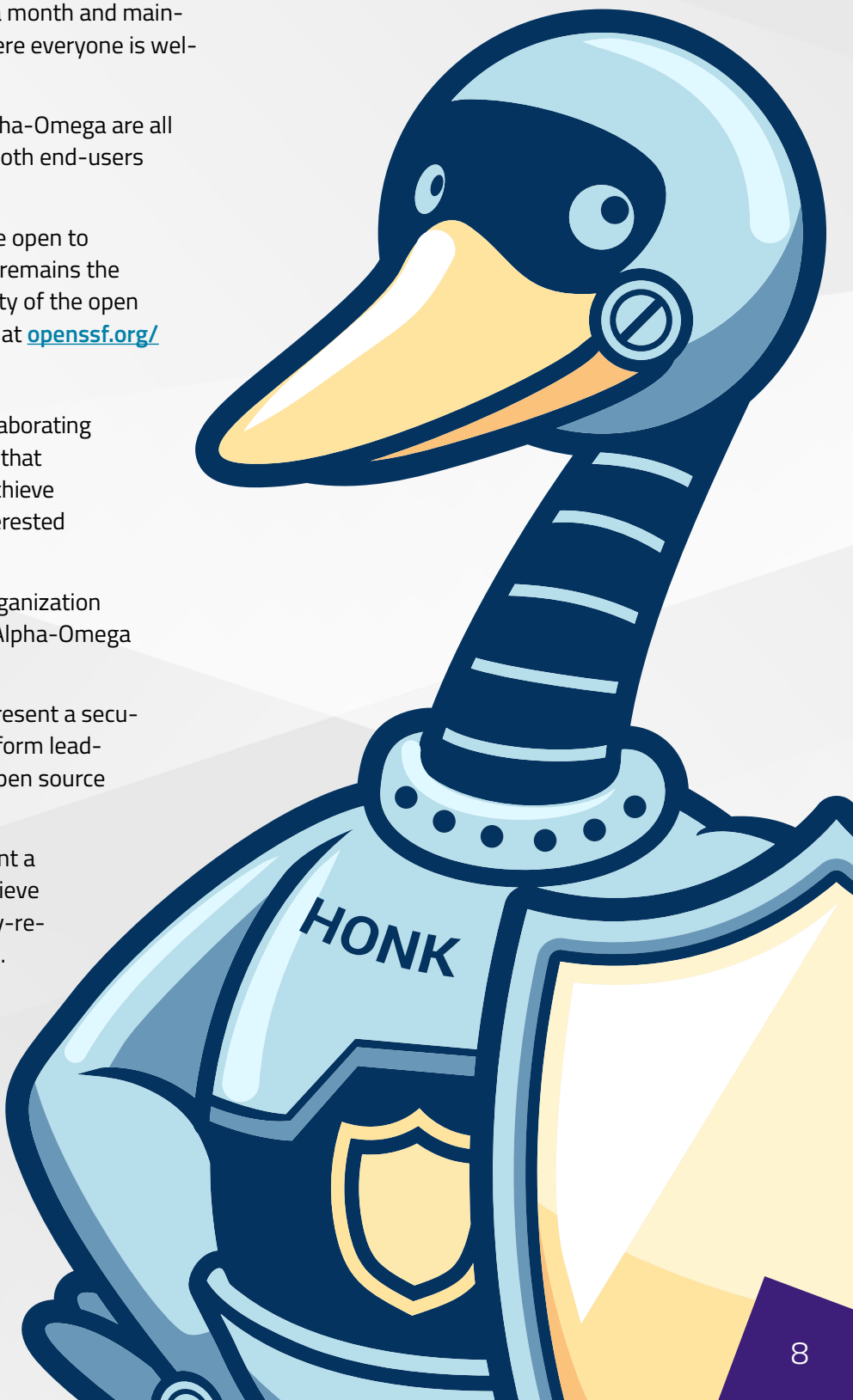
Getting Involved

The Alpha-Omega team welcomes active community participation through a few different vehicles:

- We hold public meetings once a month and maintain a public Slack channel where everyone is welcome to participate.
- The tools created as part of Alpha-Omega are all open source and available for both end-users and contributors.
- All OpenSSF working groups are open to anyone; getting involved there remains the best way to improve the security of the open source ecosystem. Learn more at openssf.org/getinvolved.

In addition, we're interested in collaborating with individuals and organizations that share our vision and can help us achieve our mission. Specifically, we're interested in these key areas:

- **Funding:** If you represent an organization able to provide funding to the Alpha-Omega project, please contact us.
- **Commercial Tooling:** If you represent a security tool or vendor that can perform leading-edge security analysis of open source projects, please contact us.
- **Critical Projects:** If you represent a critical open source project, believe you have an actionable security-related project, please contact us.



Alpha

The Alpha "half" of Alpha-Omega provides funding and other resources to the most critical open source projects, to better understand their security posture and make security improvements that benefit the end-users of those projects. Alpha is about building relationships and working collaboratively to forge a future where stakeholders can have confidence that these projects continually meet a high security bar.

How We Choose Projects to Fund

Toward achieving the vision of Alpha-Omega, we fund work around critical open source projects that, if funds were available, could make rapid progress toward improving their security posture. Both sides of this are important; we want to direct our limited resources to have the most impact on society, and we want to see that impact demonstrated quickly.

There is no shortage of critical projects, and we aren't convinced there's a way to quantifiably measure the criticality of projects below a certain level of granularity. *Is Node.js more or less critical to the open source ecosystem than Python? Is GCC more or less critical than React?* While it's an interesting area of research, we don't think it's an important question for us to try to answer; those projects are *all* critical, and we should consider funding each of them. That said, we leverage the work of the Securing Critical Projects working group to ensure we remain informed by and focused on the set of critical projects.

From there, we look for points of leverage and "shovel readiness". This has led us to investments in both ecosystems like Rust and foundations like the Eclipse Foundation, where improvements affect a disproportionate number of end-users. In general, these organizations already have relationships with security talent and the ability to hire and manage their work. This approach allowed us to do more with fewer resources within the Alpha-Omega project.

RELATIONSHIP WITH THE SECURING CRITICAL PROJECTS WORKING GROUP

From inception, we wanted the Alpha-Omega project to be closely aligned with the Securing Critical Projects working group. We asked that working group to assemble a list of the 100 most-critical open source projects to inform and guide our decision making about which projects to approach.

From that list, we've invested in Node.js, the Python Software Foundation (which maintains CPython) and the Rust Foundation (which maintains the Rust compiler and standard library). While we've chosen other projects (Eclipse Foundation and jQuery) based on additional factors, we remain committed to leveraging the output of the working group as a key part of our selection process.

Omega

Through Omega, we identify critical vulnerabilities across a wide swath of critical open source projects, and we work collaboratively with maintainers to understand those vulnerabilities and issue fixes where appropriate. We do this through automation (tools) and expert analysis (triage).

Omega is based on the hypothesis that critical vulnerabilities can be found effectively and efficiently and can scale at least linearly with the right combination of people and technology.

How We Choose Projects

Omega targets the top 10,000 most-critical open source projects, and we use two primary data sources to generate that list:

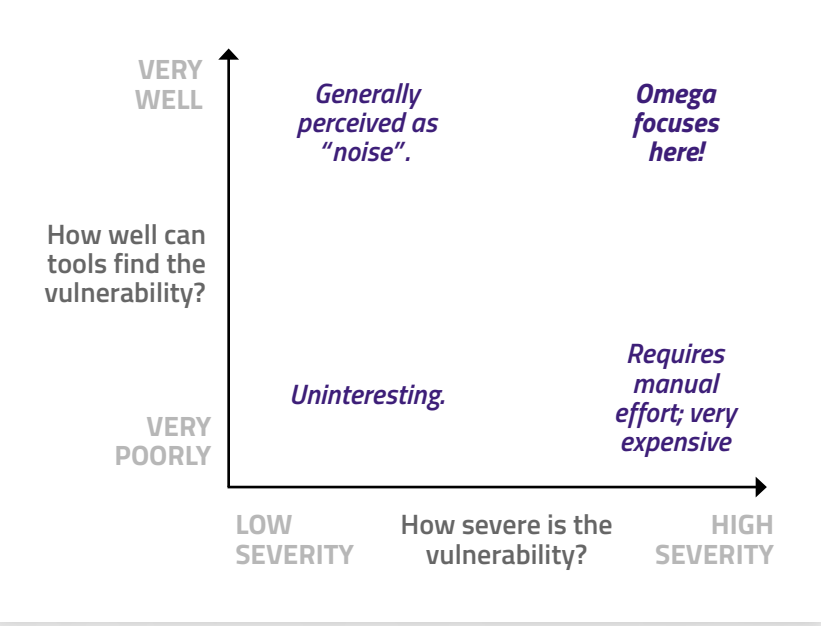
- Top 100 List: This list is manually assembled by the OpenSSF Securing Critical Projects working group.
- **OpenSSF** Criticality Score **Project**: We look at the top 10,000 most-critical projects as defined in this list.

However, if our analysis happens to include other projects that are widely-used but not technically on either of these lists, we'll often triage and report anyway. We aren't going to "forget" we saw a vulnerability if the project wouldn't otherwise qualify.

We generally look for critical vulnerabilities like code injection and avoid triaging low-confidence or low-severity findings. However, since severity is often context-dependent, we may include some lower-severity vulnerabilities when the impact of the vulnerability isn't clear.

Since Omega depends on leading-edge security tools, one of our goals is to improve tools to better identify more critical vulnerabilities with fewer false positives. In the chart to the right, this means moving more findings from the bottom right to the top right corner.

Omega remains highly experimental; we aren't sure how to most effectively deploy tools and security researchers to identify vulnerabilities at scale, but we're confident that we'll learn quickly, iterate, and improve significantly over the coming months.



Secure Open Source Rewards

In July 2022, we announced that the Secure Open Source Rewards project, funded and managed by Google, would become part of the Alpha-Omega project. Secure Open Source Rewards (or sos.dev) provides a mechanism for individuals to earn monetary rewards by contributing security improvements to critical open source projects. Secure Open Source Rewards complements the other parts of Alpha-Omega because it provides a flexible, loosely-coupled way for *anyone* to contribute to our mission.

As we enter 2023, we plan to investigate ways to better align Secure Open Source Rewards with the rest of Alpha-Omega.

Key Results

Project Bootstrapping

We started off the year bootstrapping the project. This meant working with dozens of individuals across multiple organizations to clarify and refine the project's mission and proposing the project to the OpenSSF TAC and Governing Board. We established a preliminary budget, outlined our first few key hires, and started to think about our initial investments. We held a few public sessions and refined our focus based on the feedback we received.

Hired a Security Researcher and Software Engineer

In order to meet Omega's goals, it's essential that we have both leading-edge tools and dedicated security researchers to identify critical vulnerabilities and communicate effectively with maintainers. As mentioned earlier, we recently welcomed our first hire, Yesenia Yser, and we're optimistic that we'll see rapid progress through the top 10,000 open source projects starting in early 2023.

Engagement: Eclipse Foundation

The Eclipse Foundation is a Europe-based not-for-profit corporation that acts as a steward for the Eclipse open source software community, including over 400 open source projects, including the Eclipse Platform (and IDE), Adoptium, and Jakarta EE.

The reasons we chose the Eclipse Foundation include:

- The Eclipse Foundation is a "center of mass" within the Java community; best practices implemented there are expected to have downstream benefits to the larger community.

> *"Software security is a never-ending process. This funding is the first step in a journey. We appreciate the support of the Alpha-Omega project, and are committed to using it effectively."*
>
> **— MIKE MILINKOVICH, EXECUTIVE DIRECTOR, ECLIPSE FOUNDATION**

- Eclipse had a clear, impactful set of activities in mind, and a security "champion" available.
- With over 500,000 packages available through Maven Central, Java is one of the largest developer communities, and the Eclipse Foundation are stewards for many projects this community relies upon.

For more information, you can view the Eclipse Foundation's monthly updates on our public GitHub repository.

Engagement: Rust Foundation

The Rust Foundation is a 501(c)(6) corporation, founded in February 2021 to support and complement Rust maintainers. As described in the Rust Foundation's September 2022 announcement, this engagement will include a security audit and threat model, as well as focus on improving security practices for Cargo and the crates.io package registry.

The reasons we chose the Rust Foundation include:

- Rust is a critical open source project (via the Securing Critical Projects working group).
- Rust is a popular, but relatively young language with a strong focus on memory safety; we hope that by supporting Rust's security vision, we can avoid some of the challenges that affect other programming languages.

> *"Security in open source has never been more prominent than it is today. At the Rust Foundation, we are committed to working with the Rust maintainer community to keep Rust secure, and we have been able to super charge that work with the generous support of the Alpha-Omega Project, which has financed a dedicated Security Engineer to conduct proactive work in the Rust ecosystem."*
>
> **— REBECCA RUMBUL, EXECUTIVE DIRECTOR, RUST FOUNDATION**

Engagement: Node.js

Node.js was our first Alpha engagement. From the OpenJS Foundation, we met with key individuals from the Node project, discussed the vision, and asked them to describe what they would want to do with a grant from Alpha-Omega.

The reasons we chose Node.js include:

- Node.js is a critical project (via the Securing Critical Projects Working Group) and was the #1 "most-critical" project defined by the OpenSSF Criticality Score project.
- Node.js is the most popular server-side JavaScript runtime, and according to Stack Overflow's developer survey, JavaScript is the most popular programming language.
- With over 2.1 million packages, npm is by far the largest open source package ecosystem. However, since npm is distinct from Node.js, and npm is owned by GitHub, and GitHub by Microsoft, funding was not directed to the npm project.
- The Node.js team was easy to work with, had a clear vision for what they wanted to accomplish, and were able to rapidly onboard security resources from NearForm and Trail of Bits to make progress rapidly.

For more information, you can view the Node.js monthly updates on our public GitHub repository.

Engagement: Python Software Foundation

The Python Software Foundation (PSF) is a 501(c)(3) non-profit corporation with a mission to promote, protect, and advance the Python programming language. The PSF maintains CPython, the PyPI package repository, and manages the PyCon conference.

The reasons we chose the Python Software Foundation include:

- Python is a critical open source project (via the Securing Critical Projects working group).
- According to Stack Overflow's developer survey, Python is the fourth most popular and the sixth most loved programming language.
- PyPI is the third-largest package repository (behind npm and Maven) with over 400,000 Python packages, growing at a rate of around 270 per day.

"Open source's success, which has made it both crucial and ubiquitous, brings with it an increased responsibility to users and contributors. The Python Software Foundation is continually looking for ways to meet and fund our community's needs for improved security and infrastructure. With the Alpha-Omega project's generous support, we're able to immediately level up our work examining and improving our security practices within Python core and across the many community packages we host on PyPI."

– DEB NICHOLSON, EXECUTIVE DIRECTOR, PYTHON SOFTWARE FOUNDATION

Engagement: jQuery

jQuery is one of the oldest and most popular front-end JavaScript libraries, used extensively throughout the most popular websites. Through this engagement, we intend to target the security quality of the core jQuery library itself, the build and deployment infrastructure responsible for getting jQuery out to developers, and the underlying challenges around encouraging developers to update to new versions of the library when available.

The reasons we chose jQuery include:

- jQuery is enormously popular, used by 77.4% of the 10 million most popular websites tracked by W3Techs.
- Many developers fail to update jQuery, with about 36% of sites using an outdated version containing at least one vulnerability (according to versions tracked by W3Techs).

jQuery is a bit different from most of our previous Alpha engagements, representing a single project with a long history. We wanted to broaden our view and learn how to work outside of foundations like Eclipse and the Python Software Foundation.

For more information, please see **the jQuery blog post announcing this engagement.**

Omega Tools Released

In August 2022, we released the first version of the Omega Analysis Toolchain ("Toolshed"). Contributed to OpenSSF by Microsoft, this toolchain executes 27 different security tools against open source packages and summarizes the results. These underlying tools include CodeQL, Semgrep, and tools from the OSS Gadget suite. The toolchain has been used to find dozens of vulnerabilities (including those discovered prior to it being contributed to OpenSSF), and we welcome contributions and use by security researchers.

In July 2022, we released an experimental syscall tracer designed to capture activity during an open source package's execution, to allow for later ad-hoc analysis.

Earlier in 2022, we made some progress on a triage portal intended to capture the results of the Omega Analysis Toolchain and manage vulnerabilities through their lifecycle. We've since decided to slow development of this tool and instead have the Omega staff work locally for the first 6-12 months; we'll re-evaluate after that time the value a centralized management portal would provide.

New Vulnerabilities Identified

Using the Omega Analysis Toolchain and related techniques, we found eleven security vulnerabilities in critical open source projects. These have each been reported privately to the maintainers of those affected projects, and in most cases, fixes have been released. Vulnerabilities identified include:

Vulnerability Identifier	Affected Project	Vulnerability Title
CVE-2022-32222	node.js	Attempt to read openssl.cnf from /home/iojs/build/ upon startup
GHSA-v78c-4p63-2j6c	moment-timezone	Cleartext Transmission of Sensitive Information in moment-timezone
GHSA-56x4-j7p9-fcf9	moment-timezone	Command Injection in data pipeline
Commit d9583d5e	JSHint	Potential code execution in JSHint via /bin/land.
Commit 750c4268	Azure Pipelines Agent	Potential code execution in Azure Pipelines Agent via whatsprintis.it.
Commit 7a45eeb9	Git	Potential crash in git when parsing invalid rebase "author-script" file.

Experiment: Commercial Tools

Since our goal is to use the very best security tools to rapidly and efficiently find critical vulnerabilities, we're constantly exploring the landscape, trying out new tools and thinking about how to best leverage them.

We'd like to express our appreciation to GitHub for providing a commercial license for CodeQL, and to Snyk for providing a license for Snyk Code, both of which allow us to more effectively analyze open source packages. As we accelerate our analysis in 2023, we'll continue to investigate and work with commercial security tools to be as effective and efficient as possible.

We'd also like to thank Munawar Hafiz from OpenRefactory, who has been working with us to analyze 100 of the most popular Python projects and triage the results. We provided feedback to the OpenRefactory team, which led to improvements to the rules and the dashboard experience.

Experiment: Fully-Automated Security Reviews

In May 2022, we experimented with generating a fully-automated security review of an open source project. We did this using the following methodology:

- Run the Omega Analysis Toolchain against an open source package, restricting results to high-severity findings from CodeQL, Detect-Secrets, NodeJSScan, and Semgrep.

- Attempt to rebuild the open source package using OSS Reproducible. This tool checks to see how closely an existing package (e.g. available on npmjs.com) can be re-generated from its purported source repository.
- Look up public vulnerabilities for the package using deps.dev, which includes CVEs and other vulnerability data sources.

If all of these checks came back "clean" (no findings), then we generated a templated report and sent it to the OpenSSF Security Reviews project. Here is a link to a sample automated security review for the npm package color-name.

We're continuing to think about the best way to scale this analysis and provide the results in a more consumable way.

Year Two and Beyond

As we enter the second year of Alpha-Omega, we want to increase our investments in improving the security of critical open source projects. We'll continue to base decisions on our core tenet of focusing on *direct* action. This means we'll prefer "shovel-ready" activities intended to meaningfully improve the security posture of critical open source projects or the open source ecosystem as a whole.

Our primary objectives for 2023 include:

- **Making security a first-class citizen in major projects' and foundations' budgets.** We'll do this by starting to progress our funding model to prefer joint efforts, where grants that support security activities come from additional (non-Alpha-Omega) sources. We'll also work with those projects and foundations to build security into their regular planning and budget cycles. We expect this to be a multi-year journey. A key metric that we'll start tracking is the amount of funds raised for security by non-Alpha-Omega sources.
- **Demonstrating measurable impact through security improvements to the projects we focus on.** We'll do this by collecting key improvements made based on the monthly reporting that Alpha engagements provide to us. Key metrics we'll start tracking include projects' SLSA levels, Security Scorecards data, and the number of vulnerabilities found and fixed over time.
- **Accelerating Omega.** With the onboarding of a Security Researcher and Software Engineer focused on Omega, we expect to deliver a scalable approach to vulnerability detection, triage, communication/reporting, and remediation. Key metrics include the number of critical vulnerabilities found and fixed across the 10,000 most-critical open source projects. As part of this, we'll look for ways to leverage additional tools (including commercial) that improve our capabilities.

- **Expanding Alpha-Omega to additional verticals.** We'll begin to expand the Alpha-Omega program to cover additional verticals (e.g. healthcare, automotive, financial services), where the set of critical projects may be very different from one to the next.

We'll continue to examine the investments we've made to date and increase investments in places where they've yielded the most impact. However, we recognize that the success we've had to date may be harder to ensure going forward; for example, we haven't proven out a model for funding security work on single-maintainer projects.

We plan to renew funding for the Alpha engagements that have demonstrated compelling results. At the same time, we will begin conversations with these projects about how they can grow to have their security practice be self-sustaining over time. Ideally, funding for these projects would be a core part of their annual budget. We're under no illusions that this will happen overnight.

We'll continue to look for opportunities to have leveraged, direct, and substantial impact on critical open source projects and the open source ecosystem.

> *"I am a big supporter of the Alpha-Omega project as a strategic project for open source software. The project directly improves the security of the open source ecosystem by partnering with community, providing results for all users."*
>
> **— JONATHAN MEADOWS, CITI**

Operationally, we'll continue to improve our reporting quality and cadence, aggregating insights from the Alpha engagements and data from the Omega team. These reports will be made public and will be discussed at the monthly public Alpha-Omega sessions.

We look forward to increasing our investments in 2023 and beyond, and improving how we "turn money into security."