In this Issue

Letter from the Executive Director

Welcome to our first member newsletter of 2019. This year SAFECode got out to a great start, designating January as the "Month of Champions." As the key part of this effort, a Member-led team of authors created and shared blog posts and podcasts detailing how to design, launch, manage and sustain an effective Security Champions program. If you missed it, visit our blog or download a complete PDF of the series here. I'd like to thank all of the authors and contributors on this series. Your hard work in putting together a full month of helpful advice will help those looking to create or scale a security culture within their development organizations. We've included an interview with some of our authors in this newsletter to highlight their effort and provide some insight for those who are curious about what it is like to volunteer on a SAFECode project.

Looking ahead, I'd like to highlight our upcoming Member Brown Bag series. This is a monthly webinar exclusively for SAFECode members that discusses a topic of interest identified by our technical contributors. We'll be kicking the series off this month with a presentation on "Detecting Backdoors in Open Source Software." See our article on Brown Bags below for more information on how to tune in, the upcoming schedule, and how to submit a topic for future consideration. We hope you'll join us.

And no February would be complete without a lot of planning for the RSA Conference. We'll be hosting planning sessions with our Board of Directors and Technical Leadership Council in conjunction with the conference. All SAFECode members are invited to join us for our annual member breakfast and meeting. Registration details are below – I hope to see you there!

-Steve

Government Affairs Corner

While December and January are sometimes quieter months in government and industry relations, there has been significant SAFECode activity this year. Here are some highlights:

After more than a year of deliberations and negotiations, the European Union reached consensus on the Cybersecurity Act, which focuses primarily on strengthening the mandate and providing more resources to the European Union Agency for Network and Information and Security (ENISA) to better support European Member States in tackling cybersecurity threats and attacks. The Cybersecurity Act also establishes an EU framework for cybersecurity certification that will be valid throughout the EU for products, processes, and services. According to the European Commission's press release, the "*creation of such a cybersecurity certification framework incorporates security features in the early stages of their technical design and development (security by design). It also enables their users to ascertain the level of security assurance, and ensures that these security features are independently verified.*" The new certification schemes will have obvious impacts on those working on software security; however, a lot of details of how they will be implemented are still to be determined. It is certainly a space worth watching and we'll keep you informed as things progress. SAFECode has been engaged with ENISA and the other EU authorities throughout the creation of the legislation and is committed to continuing to help inform the process as it moves forward.

In the U.S., SAFECode was invited to present at the winter meeting of the Software and Supply Chain Assurance Forum (SSCA). Co-led by the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Department of Defense (DoD), and the General Services Administration (GSA), the SSCA Forum provides a venue for government, industry, and academic participants to share knowledge and expertise on software and supply chain risks, effective practices and mitigation strategies, and related tools and technologies. All of the publicly available presentations from the winter meeting are available here. SAFECode is a frequent presenter and contributor to the SSCA Forum and looks forward to continued collaboration with this important set of supply chain security stakeholders. To be kept informed of future SSCA Forum meetings and new publications, you can sign up for the sw.assurance mailing list, operated by NIST, by sending a blank email to sw.assurance-join@nist.gov

Lastly, in industry news, the PCI Security Standards Council published new requirements for the secure design and development of payment software: the PCI Secure Software Standard and the PCI Secure Lifecycle (Secure SLC) Standard. These will be part of the new PCI Software Security Framework launching later in 2019. The PCI Secure Software Standard outlines security requirements and assessment procedures to help ensure payment software adequately protects the integrity and confidentiality of payment transactions and data. The PCI Secure SLC Standard outlines security requirements and assessment procedures for software vendors to validate how they properly manage the security of payment software throughout the entire software lifecycle.

SAFECode was invited to share its expertise in secure software development as part of the PCI standards development process. We are pleased to see that the published standard reflects an adaptation of software security best practices to the needs of the payment card industry and that the certification process is well aligned with SAFECode's principles and the concepts in SAFECode's Fundamental Practices for Secure Software Development. In particular, the standard emphasizes integrating security into the software development process rather than attempting to assure security by after-the-fact testing.

New Brown Bag Sessions Announced

Join SAFECode each month for a virtual member lunch (or breakfast or dinner depending on your timezone!) to learn more about the software and supply chain security topics that are currently top of mind with our technical contributors. All sessions are one hour in length and include plenty of time for Q&A; and discussion.

If you are interested in proposing a topic or hosting a session, submit your proposal to info@safecode.org and we'll be in touch.

February: Detecting Backdoors in Open Source Software

- Speaker: Sam Vaughan, Microsoft Customer Security & Trust – Engineering
- Date/Time: February 13, 2019 at 11 a.m. ET
- Attempts to backdoor popular open source components like NPM and PyPI, along with attacks on Docker and Debian Aptitude repositories are on the rise. We started looking for ways to identify and protect Microsoft from these types of attacks. Through our research, we demonstrated a low-cost solution to identify patterns that could be indicators of backdoor behavior but discovered that this was not sufficient to determine backdoor intent vs. insecure coding.
- In this presentation, we'll define our working definition of a backdoor, summarize our work to date, the focus of our next phase of research and solicit feedback and input for future research.

March: Choosing More Secure Open Source: Lessons From the Real World

- Speaker: Miki Demeter – Intel Product Assurance & Security, Security Researcher
- Date/Time: March 27, 2019, 11 a.m. ET
- Every day developers look on the web to find open source software to perform tasks. We always know that someone has written it already so we should just reuse it. But many of the developers of these packages tell us right from the beginning not to use the software they have written. This presentation will show how taking a few minutes up front and doing a tiny bit of due diligence will save you engineering hours on the backend… Lessons from the real world.

April: "How To Use Dynamic Languages Safely"

- Speaker: Miki Demeter – Intel Product Assurance & Security, Security Researcher
- Date/Time: April 23, 2019, 11 a.m. ET
- Today's fast-paced development environment using Python, Node.js (and others) is a path fraught with danger. From uncurated repositories to small packages pulling in hundreds if not thousands of dependencies, there is a need to be more aware of the potential dangers. Years ago, left-pad on npm was removed by a developer which ultimately brought down high profile projects around the world. Three years later, malware was injected into a library that affected thousands of additional projects. This webinar will show you how you can take steps to lower the risk of attacks on your projects.

Software Security: It Takes a Champion

January was designated SAFECode's "Month of Champions." A team of Member contributors created and shared best practices on building and sustaining an effective software security program. These insights should be of interest to anyone working to build a more security-supportive culture within their development organizations – whether they already have an established SC program, are considering implementing one, or aren't sure where to begin. For the first time. If you missed it you can catch up by visiting the SAFECode blog or by downloading a short guidebook that captures all the articles published last month. Be sure to check out our author podcasts here and here too!

Team in Focus: Meet Our Champions

SAFECode would like to recognize and thank the following Member contributors for all of their hard work on the successful Security Champions project: Vishal Asthana, Security Compass (former); Manuel Ifland, Siemens; John Martin, Boeing; Altaz Valani, Security Compass; Tania Ward, Dell; Nick Ozmore, Veracode; Kristian Beckers, Siemens; and Izar Tarandach, Autodesk.

Ever wonder what it is like to work on a SAFECode project team? Two of our Champions – Vishal Asthana and Altaz Valani were kind enough to participate in a short Q&A; about their experience working on the Security Champions and other SAFECode projects. Read the full interview here.

SAFECode: Get Involved

There are lots of ways to get involved. Whether you have one hour or 10, are looking to share information or gain it, or just want to meet others who do what you do – we have a place for you. Joining a SAFECode working group or project team provides a unique opportunity to meet your industry peers, collaborate on technical challenges, guide SAFECode's focus areas, and support continued professional development. Reach out to us at info@safecode.org for more information on how to join an existing active project or proposing a new effort.

DEVSECOPS:
SAFECode recently teamed up with the Cloud Security Alliance (CSA) to launch a new working group that will tackle issues related to DevSecOps. The working group will work to create a transparent and comprehensive management lifecycle that leverages all the components of DevSecOps to ensure timely and full functioning application deployment with security development practices integrated at every stage.

BY THE NUMBERS:
Join this group to help develop and conduct member company surveys regarding secure development practices, the findings of which will be published in an annual report and will feed the idea hopper. The team is currently focused on characterizing through data, member company's secure development training/learning programs.

FUZZING EMBEDDED SYSTEMS:
Join this group to discuss Fuzzing, an effective technique for finding robustness and resiliency issues in software that may have security implications.

Join us in Our Online Community!

Want to get more involved? SAFECode uses an interactive online forum as the home base for our Member collaboration. If you're interested in joining us online, please contact us at info@safecode.org.

Latest SAFECode Reads

- Security Champions Podcast: Final Thoughts
- Defining Success: Is Your Security Champions Program Working?
- Kicking off and Keeping up with a Security Champions Program
- Warning: Six Signs your Security Champions Program is in Trouble
- How to Build an Effective Security Champions Program
- Security Champions Podcast: The Importance of Security Champions
- Putting a Face to Software Security Champions
- Building Secure Software: It Takes a Champion
- Start 2019 Strong: Join SAFECode for our Month of Champions

Did someone forward this to you? Make sure you don't miss the next issue by subscribing today!

About This Newsletter

This newsletter is provided as a benefit to members, as it contains crucial information on upcoming industry events, opportunities for involvement in forwarding the SAFECode mission, and various channels through which SAFECode and its member companies are represented. We invite you to participate in all the above discussions and events and to forward this email to your co-workers within your company.

www.safecode.org