What's New: September 2021

SAFECode Tackles the Cybersecurity Executive Order

The President's Executive Order (EO) on Improving the Nation's CyberSecurity directed NIST and other agencies to solicit input from the private sector, academia, and government agencies to identify existing or develop new standards, tools, best practices, and other guidelines to enhance software supply chain security. In developing guidance under the EO, NIST is building on the Secure Software Development Framework (SSDF) that was released in the spring of 2020 and reflects significant contributions by SAFECode and BSA | The Software Alliance.

The initial NIST guidance on software security testing practices was released in July. This guidance goes beyond testing and reflects many secure development practices from the SSDF as well as significant input from SAFECode. https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or

The EO has established the following timeline for the cybersecurity guidelines:

- *By November 8, 2021*: NIST is to publish preliminary guidelines, based on stakeholder input and existing documents for enhancing software supply chain security.
- *By February 6, 2022*: NIST will issue guidance that identifies practices that enhance software supply chain security, including standards, procedures, and criteria.
- *By May 8, 2022*: NIST will publish additional guidelines, including procedures for periodically reviewing and updating guidelines.

SAFECode has some excellent cybersecurity resources to help your organization prepare for upcoming guidelines, including our recent SAFECode blogs and whitepapers on fuzzing and threat modeling - two practices recommended by NIST.

Help Us Change the World!

DevSecOps: SAFECode's collaboration with CSA has been reinvigorated and is currently looking for volunteers to work on the following topics: "Pragmatic Implementation," "Training & Process Integration," and "Measure, Monitor, Report, and Action." If you are interested, please reach out.

Code Integrity: Best practices for protecting source code and build system

Recent attacks against SolarWinds or ASUS show that a secure development lifecycle is not sufficient to prevent code from being exploited. Technology vendors also need to employ best practices to ensure that malicious code is not being inserted into the code they create for their customers. The goal of the working group is to discuss best practices to ensure code integrity during the code development or delivery process.

Hybrid Work-Force: What does this mean for secure software development?

As countries continue with their mass vaccination programs, some organizations are considering a mandated "back to office" lifestyle for their employees. The rationale cited is their inability to manage security with a large remote workforce. Other organizations are planning to let their employees choose whether to work from home or the office. Come and participate in an exploratory discussion on what a hybrid workforce means for the governance and implementation of secure software development. The next steps, if any, will be determined based on this initial exploration.

The Benefits of Being a SAFECode Volunteer

- Participate in shaping the content of SAFECode publications
- Give back to the community by sharing your knowledge
- Improve the quality of blogs, papers, training, and more
- Change the World!

What do I do next? Let us know you'd like to get involved by signing up **here**. You can also forward this request to colleagues in your company that are experts in any of these areas.

Share your interest

Projects in Flight

DevSecOps

SAFECode is in a partnership with CSA to create a comprehensive software development and security management lifecycle that leverages principles and best practices of DevSecOps and Security Champions.

OSSF Working Group

This group will help to shape how SAFECode will continue to contribute to the OSSF's work.

Code Integrity

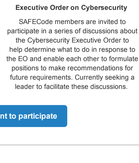
Recent attacks against SolarWinds or ASUS show that a secure development lifecycle alone is not sufficient to prevent code from being exploited.

Post Quantum Crypto

This working group is focused on the implications of post-quantum algorithms for developers and offers guidance on preparing for a smooth transition.

Open Source Security Foundation

SAFECode is a member of the OSSF under the Linux Foundation.



Executive Order on Cybersecurity

SAFECode members are invited to participate in a series of discussions about the Cybersecurity Executive Order to help determine what to do in response to the EO and enable each other to formulate positions to make recommendations for future requirements. Currently seeking a leader to facilitate these discussions.

I want to participate

In Case You Missed It

Our most recent Post Quantum Crypto blog series provides guidance on developing a comprehensive Crypto Agility strategy. Understand how to design, implement and validate cryptography for your organization's benefit.

Read the blog

Please forward this messaging to your colleagues at your organization. If you have any questions, please contact us at helpdesk@safecode.org

Visit safecode.org