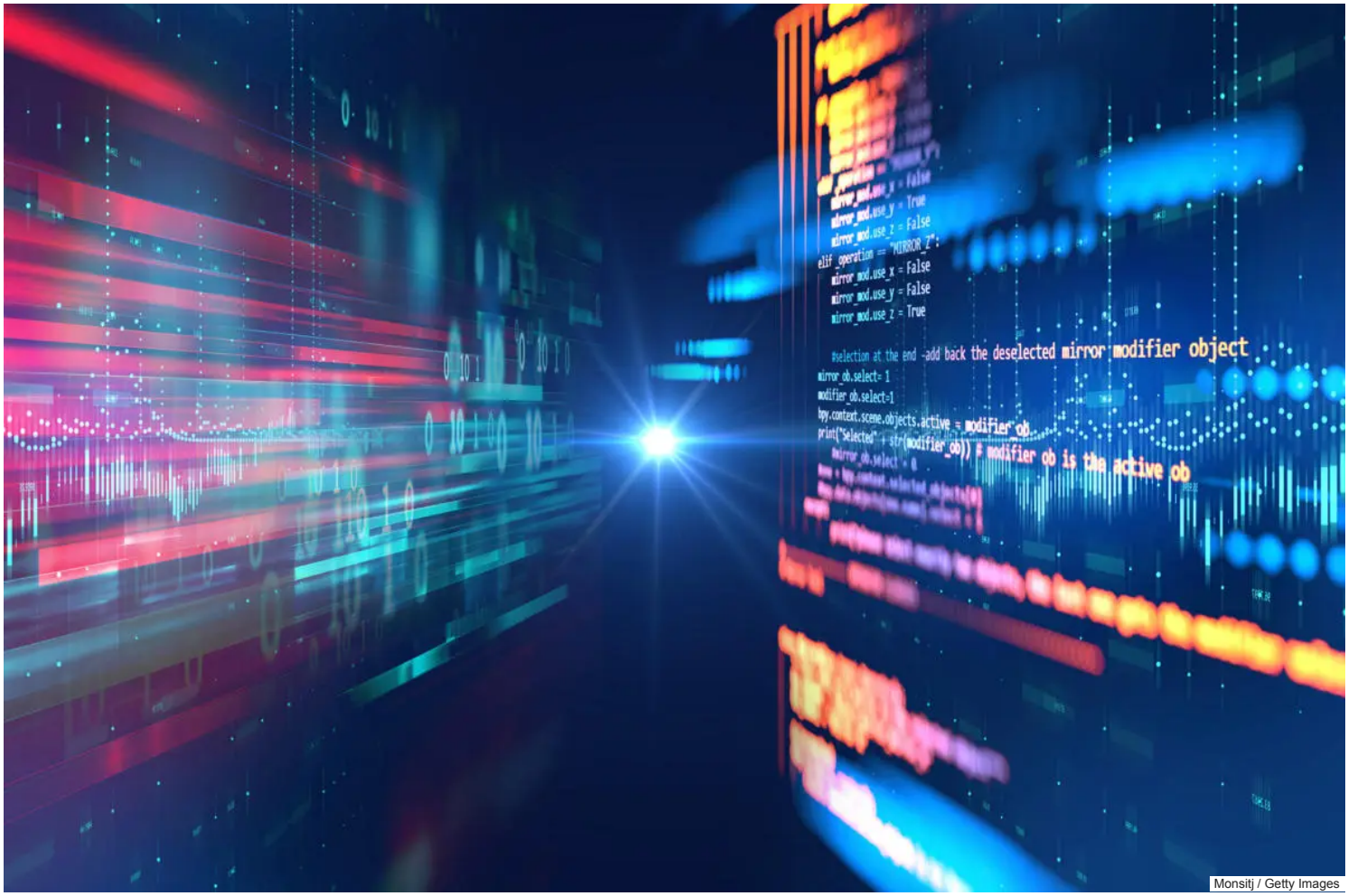
FEATURE

8 notable open-source security initiatives of 2022

Vendors, collectives and governments are contributing to improve the security of open-source code, software, and development amid organizations' increasing use of open-source resources.



Monsitj / Getty Images

By Michael Hill
UK Editor, CSO
SEP 12, 2022 2:00 AM PT

Open-source security has been high on the agenda this year, with a number of initiatives, projects, and guidance launched in 2022 to help improve the cyber resiliency of open-source code, software and development. Vendors, tech firms, collectives and governments have contributed to helping raise the open-source security bar amid organizations' increasing use of and reliance upon open-source resources, along with the complex security risks and challenges that come with it.

"2022 has intensified the necessary focus on the important topics of open-source security, including supply chain security. It has also accelerated efforts to identify what was left to do, and then start doing it. In sum: things are just getting started, but progress has been made," David A. Wheeler, director of open-source supply chain security at the Linux Foundation, tells CSO.

Content Continues Below

look inside, open-source software (OSS) components. That's not a problem per se – OSS enables an incredible number of goods and services – but it's a problem if the OSS is vulnerable to attack." To cause any change, organizations need resources, including people's time and money, he adds. "Some actions won't require much, but you still often need some as a catalyst. Some will require more resources because the software industry is large, and the amount of software is huge. For many developers, 'make it secure' is a new, unanticipated requirement."

Here are eight notable open-source security initiatives of 2022.

The White House hosts open-source security summit

In January, The White House convened government and private sector stakeholders to discuss initiatives to improve the security of open-source software and new approaches to collaboration to drive improvements. Meeting participants included Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger and National Cyber Director Chris Inglis, along with representatives from tech firms including Akamai, Amazon, Apple, Cloudflare, Facebook/Meta, the Linux Foundation, the Open Source Security Foundation (OpenSSF), and Microsoft.

Content Continues Below

"Participants had a substantive and constructive discussion on how to make a difference in the security of open-source software, while effectively engaging with and supporting, the open-source community," a White House readout stated. "The discussion focused on three topics: preventing security defects and vulnerabilities in code and open-source packages, improving the process for finding defects and fixing them, and shortening the response time for distributing and implementing fixes."

All participants will continue discussions to support these initiatives in the coming weeks, which are open to all interested public and private stakeholders, it added.

OpenSSF,Linux Foundation publish Open Source Software Security Mobilization Plan

In May, the OpenSSF and the Linux Foundation published The Open Source Software Security Mobilization Plan, outlining a 10-stream strategy with steps for immediate and long-term improvements within open-source software for both underlying components and operation. Its three core security aims are:

- Securing open-source software production by focusing on preventing security defects and vulnerabilities in code and open-source packages.
- Improving vulnerability discovery and remediation by enhancing the process for finding defects and fixing them.
- Shortening ecosystem patching response times by quickening the distribution and implementation of fixes.

Content Continues Below

"Vulnerabilities and weaknesses in widely deployed software present systemic threats to the security and stability of modern society as government services, infrastructure providers, non-profits, and the vast majority of private businesses rely on software in order to function," the OpenSSF wrote. The time has come to apply security best practices to the whole of the software ecosystem, including open source, encompassing a more comprehensive series of investments to shift security from a largely reactive exercise to a proactive approach, it added.

JFrog introduces Project Pyrsia to secure open-source software packages, binary code

In May, JFrog announced the launch of Project Pyrsia, a decentralized, secure build network and software package repository that uses blockchain technology to secure open-source software packages from vulnerabilities and malicious code. It is aimed at helping

needing to build, maintain, or operate complex processes for securely managing dependencies," JFrog said, stating that the framework will help provide:

- An independent, secure build network for open-source software
- Trustworthiness of software packages
- Completeness of known open-source software dependencies

"At JFrog we believe open-source security will only be successful if we provide the community with the same tools and services that are available to enterprises," commented Stephen Chin, VP of developer relations at JFrog. "The combination of an open-source, customizable architecture, and a robust, active community makes Pyrsia the most transparent and trustworthy way to obtain secure software packages."

Content Continues Below

OpenUK launches Summer of Open Source Security

In June, OpenUK launched the Summer of Open Source Security, a two-month-long initiative featuring events, talks, and podcasts dedicated to open-source software security and supply chain management. Conversations included contextualizing the positioning of governments and enterprises across the globe with regards to national critical infrastructure built on open-source software and recognizing the need to consider maintenance, security, and the curation of open-source software.

"Open source differs greatly from proprietary software, in part in the proprietary royalty model and the co-related exclusion of liability. This directly impacts the basis of the balance of risk which is very different for open source and proprietary software. The quid pro quo for the free distribution of the open-source code is the absolute wavier of liability," wrote OpenUK CEO Amanda Brock.

GitGuardian announces ggcanary project to detect open-source software risks

In July, code security platform provider GitGuardian announced the launch of an open-source canary tokens project to help organizations detect compromised developer and DevOps environments. The firm said the ggcanary project is designed to help businesses detect compromises quicker and is built with the following features:

- Reliance on Terraform, using the popular infrastructure-as-code software tool by HashiCorp to create and manage AWS canary tokens
- Highly sensitive intrusion detection that uses AWS CloudTrail audit logs to track all types of actions performed on the canary tokens by attackers
- Scalability of up to 5,000 active AWS canary tokens deployed on the internal perimeter of an organization, in source-code repositories, CI/CD tools, ticketing, and messaging systems such as Jira, Slack, or Microsoft Teams
- Its own alerting system, integrated with AWS Simple Email Service (SES), Slack and SendGrid. Users can also extend it to forward alerts to SOCs, SIEMs, or ITSMs

Content Continues Below

Google launches open-source software vulnerability bug bounty program

In August, Google launched the Open Source Software Vulnerability Rewards Program (OSS VRP) to reward discoveries of vulnerabilities in Google's open-source projects. In a blog post, Google wrote that its OSS VRP encourages researchers to report vulnerabilities with the greatest real, and potential, impact on open-source software under the Google portfolio, focusing on:

- All up-to-date versions of open-source software (including repository settings) stored in the public repositories of Google-owned GitHub organizations
- Those projects' third-party dependencies (with prior notification to the affected dependency required before submission to Google's OSS VRP)

submissions of:

- Vulnerabilities that lead to supply chain compromise
- Design issues that cause product vulnerabilities
- Other security issues such as sensitive or leaked credentials, weak passwords, or insecure installations

Rewards range from $100 to $31,337 USD, depending on vulnerability severity and project importance, Google said.

CISA, NSA release security guidance for open-source software supply chain

In August, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. National Security Agency (NSA) published guidance advising developers how to better secure the U.S. software supply chain, with a significant focus on open-source software.

“Development organizations should employ dedicated systems that download, scan, and perform recurring checks of open-source libraries for new versions, updates, and known or new vulnerabilities,” the guidance read. “As with all software, we strongly recommend educating developers on considerations for the use of open-source software, close-source software, and evolving best-practice mitigations.”

The management team should also establish, manage, and apply release criteria relating to open-source software, the guidance added, ensuring that all shipping of open-source meets company-wide standards, including vulnerability assessment of the source. “Ship the latest stable versions of open-source, removing or providing a support plan for any open-source software that has reached end of life, and ensuring licensing, if any, is fully understood and compliant with the open-source usage policy,” the guidance stated.

OpenSSF publishes npm best practices to help developers tackle open-source dependency risks

In September, the OpenSSF released the npm Best Practices Guide to help JavaScript and TypeScript developers reduce the security risks associated with using open-source dependencies. The guide is a product of the OpenSSF Best Practices Working Group and focuses on dependency management and supply chain security for npm. It covers various areas such as how to set up a secure CI configuration, how to avoid dependency confusion, and how to limit the consequences of a hijacked dependency.

Speaking to CSO in September, the Linux Foundation’s Wheeler said the biggest security risk posed by developers’ use of open-source dependencies is underestimating the effects that vulnerabilities in both direct and indirect dependencies can have. “Flaws can crop up in any software, which can significantly impact the supply chain that uses it if care is not taken. Too often, many of the dependencies are invisible and neither developers nor organizations see all the layers to the stack. The solution isn’t to stop reusing software; the solution is to reuse software wisely and to be prepared to update components when vulnerabilities are found.”

[Learn how to track and secure open source in your enterprise. | Get the latest from CSO by signing up for our newsletters.]