NEWS FEATURE 8 FEB 2024

How to Navigate Open-Source Security Without Stifling Innovation

James Coker
Deputy Editor, Infosecurity Magazine
Follow @ReporterCoker

Government interest in open-source software security is on the rise and reflects the scale upon which this code is utilized across all sectors, including critical infrastructure.

The widespread usage of open-source software, and the risks it poses, was highlighted by the notorious Log4j vulnerability that was discovered in December 2021 and is believed to have impacted 58% of organizations globally.

Speaking during the State of Open Con 2024 (SOOCon24) event in London, Rebecca Rumbul, CEO of the Rust Foundation, noted that conversations between the open-source community, the cybersecurity industry and governments simply did not take place three years ago. Now, they are happening on a regular basis.

However, there are concerns that security diktats issued by governments on this domain could damage the huge benefits open-source software provides – in particular, innovation, cost and transparency. This is encapsulated by opposition

from this community to provisions set out in a draft version of the EU's Cyber Resilience Act last year.

Here are four ways open-source software security can be enhanced without impacting the benefits it provides:

1. Governments Must Engage With Open Source Issues Appropriately

Top-Down Legislation Doomed to Fail

Governments simply imposing legislation on the community will be ineffective in improving open-source security, and potentially damaging, argued some SOOCon24 speakers.

This is because the open-source software community does not have the top-down structure of traditional organizations – it is an ecosystem of individuals, many of whom develop and maintain code in their spare time.

Controls like software bills of materials (SBOMs) and software development lifecycle (SDLC) are harder to enforce on open-source development compared to software created in public and private sector organizations.

Victoria Ontiveros, Vulnerability Analyst at the Cybersecurity and Infrastructure Security Agency (CISA), acknowledged there has traditionally been a

misunderstanding of the open-source ecosystem at government level.

“We need to change how we communicate with the open-source community,” Ontiveros noted.

Omkhar Arasarantnam, General Manager at OpenSSF, said that there is a willingness to listen and improve security from within the open-source community, as long as governments approach the issue with the appropriate care and attention. He said the emphasis should be on building the code correctly from the beginning.

“Let’s put aside political difference and focus on technical correctness,” he outlined.

UK and US Leading With Open-Source Engagement

There has been a growing willingness among regulators, particularly from the US and UK, to reach out to the open-source community, including associations like the Rust Foundation.

“The openness of agencies like CISA to work with us and not against us, is really heartening,” Rumbul told *Infosecurity*.

The Rust Foundation is an independent nonprofit dedicated to the safety, security, sustainability, and health of the Rust Programming language and the people who use it.

Rumbul also praised the EU’s engagement with the open-source community to improve the relevant provisions in the EU Cyber Resilience Act (CRA) following concerns with the earlier draft. A public letter signed by prominent members of the open-source community warned that the wording was too broad and would significantly hamper its ability to innovate, causing a significant economic impact.

“The state of the CRA now, in its finalized form, is substantially better than when it was first released last year,” she said.

This approach will enable governments to “regulate well, for the benefit of everyone.”

Amanda Brock, CEO of OpenUK, told *Infosecurity* that the US and UK governments are spending time to understand the nuances of the ecosystem before taking regulatory action. This is in contrast to the top-down approach the EU took in the initial drafting of the CRA.

This involves “consulting, understanding how things work, rather than legislating before they are clear,” she said.

2. Open-Source Developers and Users Need More Cybersecurity Education

Security Training Must Be Mandatory for Developers

A lack of security training for developers is a major barrier to ensuring security by design principles are embedded into open-source software development.

"The openness of agencies like CISA to work with us and not against us, is really heartening"

Rumbul acknowledged: "Security isn't a big component at all when you're learning to code."

Developer education needs to come from a variety of sources and be a continuous process.

This starts in the education system. In 2023, the CISA Director Jen Easterly called for universities to include security as a standard element in computer science coursework.

Industry associations like the Open Source Security Foundation (OSSF) also provide free security education for developers.

Additionally, the process of building security into code should be made as seamless as possible, argued Rumble.

"What we're trying to do in the Rust ecosystem is develop tooling, processes and automation that means that they don't have to take an extra step or be prescriptive about them having to do extra things," she explained.

Organizations Must Understand the Risks of Using Open Source

Education on open-source security should extend beyond developers to the users themselves. This is to ensure organizations understand the risks involved with using open-source code and how to mitigate them.

Ontiveros said that the US government is prioritizing securing open-source software used in critical infrastructure, such as water plants.

"We need to work with the critical infrastructure industry so they know that they have open-source dependencies and how to manage these risks," she outlined.

In October 2023, the US government issued guidance on securing open-source software (OSS) in operational technology (OT) critical infrastructure environments.

OpenSSF's Arasarantnam added that organizations should also recognize that security incidents will occur from open-source code vulnerabilities.

Therefore, firms must establish a "well-practised and boring" way to handle the incident.

3. Increase Open-Source Code Transparency

Open-source security would be significantly enhanced by a culture of developers "writing stuff down," according to Stephen Augustus, Head of Open Source at Cisco.

This includes information on dependencies, how recently the library was released and whether there are active maintainers who can be contacted.

This would help organizations make better security-centric decisions on using particular open-source code in their software.

"Start locally and build up a corpus of work that allow people to reflect on whether or not something is a good dependency," said Augustus.

This was a sentiment echoed by Ontiveros, who emphasized the importance of SBOMs in demonstrating the origins of software components. "You can make risk management decisions based on that information," she said.

"Put your SBOMs somewhere everyone can find it so that future users down the road can make their decisions based on all the information," added Ontiveros.

4. Take Ownership for Open-Source Security

End-Users Are Accountable Too

All stakeholders in the open-source ecosystem should take ownership of security and not simply expect this to be managed by the developers.

"If you're packaging software for millions of people, you need to have a high degree of certainty rather than relying on Mother Nature to make it secure," said Arasarantnam.

Organizations benefit from the free code they get from the open-source community. As a result, they should also accept accountability for any security issues that arise.

Governments Should Provide Financial Support to Open-Source Ecosystem

Governments are among the biggest consumers of open-source software in the world and should be supporting the ecosystem financially.

Rumbul argued they have a particular responsibility to lead the way in open-source security best practices and help fund the security maintenance of the ecosystem.

“I would love the government to not just regulate, but financially support the work we are doing because they are consumers of it,” she commented.

Brock emphasized that government departments must increase their understanding of open-source software to do so.

“It’s so fundamental to the infrastructure that we really need them to get up to speed quickly,” she said.

You may also like

NEWS 8 FEB 2023

#SOOCon23: Global Cooperation Needed to Enhance Open Source Software Security

NEWS 1 MAY 2013

Three-fourths of organizations lack app component policy

NEWS 30 OCT 2013

Building Security In Maturity Model: Version 5 Released

NEWS 20 JUL 2012

A new cyber security challenge for system developers

NEWS 13 NOV 2009

Microsoft gets agile with Security Development Lifecycle

What's hot on Infosecurity Magazine?

Read | Shared | Watched | Editor's Choice

1

NEWS FEATURE 12 DEC 2023

Top 10 Cyber-Attacks of 2023

2

NEWS 6 FEB 2024

Safer Internet Day: Two Million Brits Victims of Financial Identity Fraud

3

NEWS 6 FEB 2024

Latest Ivanti Zero Day Exploited By Scores of IPs

4

NEWS 7 FEB 2024

Ransomware Payments Hit $1bn All-Time High in 2023

5

NEWS 7 FEB 2024

Meta to Introduce Labeling for AI-Generated Images Ahead of US Election

NEWS 5 FEB 2024

6

Clorox and Johnson Controls Reveal $76m Cyber-Attack Bill

Infosecurity Magazine

The magazine

About Infosecurity
Meet the team
Contact us

Advertisers

Media pack

Contributors

Forward features
Op-ed
Next-gen submission