

Latest

Cyber Insurance, A Must-Have for Small Businesses

News Topics Features Webinars White Papers Podcasts Events & Conferences Directory

INFOSECURITY MAGAZINE HOME » OPINIONS » THE SECURITY CHALLENGE OF OPEN SOURCE SOFTWARE

7 FEB 2023 OPINION

# The Security Challenge of Open Source Software



Amanda Brock CEO, OpenUK

Open-source software forms the heart of today's digital services, underpinning our public services and critical infrastructure. It creates the building blocks for applications, services and the underlying infrastructure in businesses and the public sector. Free-to-use, open-source software is a digital public good benefiting us all.

However, understanding how open-source software should be curated by the user to support those requirements is limited. Curation involves more than managing software from a technical perspective; rather, it broadly covers good governance and practices in open-source software usage. Curation varies depending on the use case of the software, and the burden of ensuring the software meets the requirements of a regulated environment sits with the end user selecting it for this use.

## Source Code Transparency

Source transparency supports a vastly better development methodology. If we can rely on the visibility of the source, we can produce a more trusted infrastructure. With open-source licensed software, a user takes code freely and chooses where to utilize it. Therefore, the user, not the developer, is responsible for its implementation.

Open-source software is open to everyone for any purpose, making it potentially vulnerable to bad actors. This perceived vulnerability is managed by security techniques to identify and manage potential bad actors in a coordinated way. All software has faults that must be fixed, but this requires resources. Therein lies the actual problem for open-source software. Open source's collaborative innovation provides free-to-use functionality that would otherwise require creation from scratch. However, projects that provide this essential and pervasive technology haven't

## Related to This Story

Europe's Open Source Bug Bounty: A Wrong Start

Ensuring Secure Practices around Open Source

Addressing Inherent Risks in Code Repositories

DHS Releases Report into Log4j Vulnerabilities and Response

#HowTo Have Better Open Source Security for the Financial Services Sector

always been supported effectively. When something goes wrong, users rely on a 'community' response – code creators, maintainers and users collaborating to fix it.

However, some projects may not have the necessary financial resources or skilled human capital. Popular projects get the most attention and resources to fix any potential issues, while lesser-known projects have inherently fewer eyes to check them. To focus more eyes on open-source projects and distribute these efforts fairly, we need more than the existing community members.

For example, Apache Log4j **was estimated** to be used by 58% of all organizations and across applications that affected millions of people. When the exploit was discovered, Cloudflare **saw** more than 1000 attempted exploits per second. Log4j was ubiquitous code and highly utilized, yet it relied on a tiny team to build and maintain the project.

The Log4Shell vulnerability has been unfairly used as a stick to beat open source – apparent inextricable proof that the 'many eyes' model offered by open source is not fit for purpose. Yet vulnerabilities occur in all software, even those maintained by private companies holding extensive resources. What matters most is how these vulnerabilities are found, fixed and then disseminated to the community that uses the project.

## Open Source and Curation

End users are not only responsible for their utilization of open-source software but receive commercial advantage from it being distributed freely and at zero cost. Therefore, they must take on a higher degree of responsibility for the utilization of that open-source code. It would be unreasonable to seek to shift any responsibility to the benevolence of these creators and maintainers.

We can't rely on the goodwill and efforts of the community alone to deliver and maintain code when it is used at the scale that open source is deployed. Support is needed from the wider enterprise software industry and governments. Google has **led the way by committing \$100m to fund more cooperation** between companies in responding to problems. This is promising, but a broader range of global corporate engagement must occur.

This should consist of financial support for those directly contributing to projects and more human resources that can work alongside those committers. The digital skills gap is growing, and more efforts are needed to develop future generations with the required skill sets around secure coding, spotting potential issues and working with communities and users to ensure updates are implemented effectively.

On the government side, the US government has developed more understanding of open-source software, built improved user practices and **mandated software bill of materials (SBOMs)** for US federal software projects. The European Commission has lifted this into its **2022 Cyber Resilience Act**. The UK government is due to release its risk-based approach in early 2023.

Open source is at a crossroads. It has become the foundation for critical services for both the public sector and private businesses. The economic downturn will only increase organizations' reliance on free software. But for open source to be secure in future, we cannot keep taking from the community and giving nothing in return. We must focus on funding and resourcing in a joined-up and collaborative way.

## What's Hot on Infosecurity Magazine?

Read Shared Watched Editor's Choice

- 1 2 FEB 2023 NEWS  
City of London on High Alert After Ransomware Attack
- 2 1 FEB 2023 NEWS  
Thriving Dark Web Trade in Fake Security Certifications
- 3 3 FEB 2023 NEWS  
MalVirt Loaders Exploit .NET Virtualization to Deliver Malvertising Attacks
- 4 3 FEB 2023 NEWS  
New Credential-Stealing Campaign By APT34 Targets Middle East Firms
- 5 3 FEB 2023 NEWS  
Quarter of CFOs Have Suffered \$1m+ Breaches
- 6 2 FEB 2023 NEWS  
Lazarus Group Attack Identified After Operational Security Fail

o Comments

 Login ▾

G

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 

Name

Share

**Best** Newest Oldest

Be the first to comment.

[Subscribe](#)

[Privacy](#)

[Do Not Sell My Data](#)

ALSO ON INFOSECURITY MAGAZINE

a month ago · 1 comment

**No Major Spike  
in Reported  
Ransomware ...**

16 days ago · 1 comment

**MFA Bypass:  
The Next  
Frontline for ...**

2 months ago ·

**How to  
Mitigat  
Cyber F**

- The Magazine
- [About Infosecurity](#)
- [Subscription](#)
- [Meet the Team](#)
- [Contact Us](#)

[Cookies Settings](#)

- Advertisers
- [Media Pack](#)
- Contributors
- [Forward Features](#)
- [Op-ed](#)
- [Next-Gen Submission](#)