# Navigating the future of open-source software security



Open-source software has permeated the technology landscape, presenting unique security challenges compared to proprietary software. Chris Hughes, chief security advisor at the open-source software security startup Endor Labs, provided insights into the current state of open-source software security and future trends during a recent conversation with TechRepublic.

Hughes elaborated on the rising adoption of open-source software (OSS), which he defined as software with freely available source code that can be repurposed for various projects, potentially under certain restrictions. He referenced a Harvard Business School study, suggesting that companies would need to invest approximately $8.8 trillion in technology and manpower to reconstruct the software infrastructure if open-source options were unavailable. According to Hughes, “the estimates are 70-90% of all applications have open source, and roughly 90% of those code bases are entirely made up of open source."

Looking ahead to 2025, Hughes predicts a landscape shaped significantly by both the increased use of open-source software and the sophistication of potential attacks on these systems. He stated that organisations would continue to implement foundational governance for OSS, improving their understanding of what open-source components are embedded within their enterprise systems. "More companies will use open-source and commercial tools to help them start to understand their OSS consumption," Hughes emphasised, highlighting an industry shift towards risk-informed OSS usage.

Another focal point in Hughes’ discussion pertains to the significant role of artificial intelligence in shaping application security and open-source practices. As AI technologies evolve, organisations are increasingly leveraging AI to scrutinise code and rectify emerging vulnerabilities. In a landscape where attackers are expected to target prevalent open-source AI libraries and projects, Hughes noted that enterprises are keenly interested in understanding the security protocols surrounding their open-source software, including maintenance practices and responsiveness to vulnerabilities.

In relation to specific incidents that underline the vulnerabilities inherent within open-source systems, Hughes referenced an attack in April 2024 where social engineering tactics compromised open-source utilities. He remarked, “that one was really kind of sinister because the open-source ecosystem is largely sustained by unpaid volunteers.” Such attacks have drawn attention to the fragility of an ecosystem reliant on voluntary contributions.

The Open Source Initiative’s October 2024 establishment of a clear definition for open-source AI, incorporating elements of freedom in utilisation, study, modification, and sharing, marks a significant development in the field. Hughes explained this categorisation is essential as distribution platforms, such as Hugging Face, grow in popularity and the origin and composition of AI models become critical questions for security teams.

In March 2024, the Cybersecurity and Infrastructure Security Agency (CISA) finalised a secure software development self-attestation form, signalling that developers of software utilised by the U.S. federal government must affirm their adherence to secure development practices. This framework may lead commercial organisations to impose similar requirements, although a level of trust remains essential in vendor relations.

Hughes asserted that merely performing software composition analysis will be insufficient as complexity within software infrastructures increases. With the number of vulnerabilities rising significantly, this growth presents challenges for developers in prioritising fixes. Companies like Endor Labs aim to simplify this process by providing insights on dependencies, both direct and indirect, within open-source code.

As the landscape of open-source software security evolves, the necessity for comprehensive governance and proactive risk management strategies becomes increasingly evident, as organisations navigate the complexities introduced by both open-source usage and evolving threats within the ecosystem.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.isms.online/information-security/securing-open-source-in-2025-and-beyond-a-roadmap-for-progress/> - This article discusses the systemic challenges facing the open-source ecosystem, including the prevalence of vulnerabilities, poor dependency management, and the risk of malicious packages. It aligns with Hughes' points on the widespread use of open-source software and the need for robust security measures.
2. <https://www.isms.online/information-security/securing-open-source-in-2025-and-beyond-a-roadmap-for-progress/> - The article highlights the importance of maintaining an inventory of open-source software, continuous patch management, and incident management processes, which are in line with Hughes' emphasis on foundational governance and risk-informed OSS usage.
3. <https://www.reversinglabs.com/blog/census-iii-study-spotlights-ongoing-open-source-security-challenges> - This study by the Linux Foundation, OpenSSF, and Harvard University underscores the security challenges in open-source software, such as backward incompatibilities and the lack of standard schemas, supporting Hughes' discussion on the complexities and vulnerabilities in OSS.
4. <https://www.reversinglabs.com/blog/census-iii-study-spotlights-ongoing-open-source-security-challenges> - The Census III study mentions the risks posed by low-staffed open-source projects, which aligns with Hughes' mention of the fragility of the open-source ecosystem reliant on voluntary contributions.
5. <https://www.isms.online/information-security/securing-open-source-in-2025-and-beyond-a-roadmap-for-progress/> - The article discusses the role of AI in enhancing security protocols for open-source software, mirroring Hughes' prediction on the increasing use of AI to scrutinise code and rectify vulnerabilities.
6. <https://www.reversinglabs.com/blog/census-iii-study-spotlights-ongoing-open-source-security-challenges> - The study highlights the need for funding open-source developers and projects, which is relevant to Hughes' discussion on the economic and resource implications of maintaining open-source software.
7. <https://www.isms.online/information-security/securing-open-source-in-2025-and-beyond-a-roadmap-for-progress/> - The article mentions the Log4j vulnerability as a case study, illustrating the complexity of dependency chains and the ongoing risks even after patches are available, supporting Hughes' points on the significance of understanding and managing open-source components.
8. <https://www.reversinglabs.com/blog/census-iii-study-spotlights-ongoing-open-source-security-challenges> - The study emphasizes the importance of standardized schema efforts and better management of open-source components, aligning with Hughes' emphasis on improving the understanding of embedded open-source components within enterprise systems.
9. <https://www.isms.online/information-security/securing-open-source-in-2025-and-beyond-a-roadmap-for-progress/> - The article discusses the need for comprehensive governance, security policies, and continuous improvement culture, which are key points in Hughes' discussion on the evolving landscape of open-source software security.
10. <https://www.reversinglabs.com/blog/census-iii-study-spotlights-ongoing-open-source-security-challenges> - The study notes the critical role of open-source libraries in infrastructure and the risks associated with their maintenance, supporting Hughes' mention of the critical nature of open-source components in modern software infrastructure.
11. <https://www.techrepublic.com/article/open-source-software-security-trends-2025/> - Please view link - unable to able to access data