Synopsys Study Shows Open Source Security Top-of-Mind but Patching Too Slow

Global survey of 1,500 IT professionals finds that 40% of respondents worldwide had delivery schedules disrupted to address open source vulnerabilities

MOUNTAIN VIEW, Calif., Dec. 8, 2020 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the report, DevSecOps Practices and Open Source Management in 2020. Produced by the Synopsys Cybersecurity Research Center (CyRC), the report highlights the findings from a survey of 1,500 IT professionals working in cyber security, software development, software engineering, and web development. The report explores the strategies that organizations around the world are using to address open source vulnerability management as well as the growing problem of outdated or abandoned open source components in commercial code.

Open source plays a critical role in today's software ecosystem. The overwhelming majority of modern codebases contain open source components, with open source often comprising 70% or more of the overall code. Yet paralleling the growth of open source use is the mounting security risk posed by unmanaged open source. In fact, according to the 2020 OSSRA report, 75% of the codebases audited by Synopsys contain open source components with known security vulnerabilities. To combat this situation, respondents to the survey cite identification of known security vulnerabilities as the number one criterion when vetting new open source components.

"It's clear that unpatched vulnerabilities are a major source of developer pain, and ultimately business risk." said Tim Mackey, principal security strategist of the Synopsys Cybersecurity Research Center. "The 'DevSecOps Practices and Open Source Management in 2020' report highlights how organizations are struggling to effectively track and manage their open source risk."

"Over half—51%—say it takes two to three weeks for them to apply an open source patch," Mackey continued. "This is likely tied to the fact that only 38% are using an automated software composition analysis (SCA) tool to identify which open source components are in use and when updates are released. The remaining organizations are probably employing manual processes to manage open source—processes that can slow down development and operations teams, forcing them to play catch-up on security in a climate where, on average, dozens of new security disclosures are published daily."

Other noteworthy findings in the "DevSecOps Practices and Open Source Management in 2020" report include:

- **DevSecOps is rapidly growing worldwide.** A combined 63% of respondents reported that they are incorporating some measure of DevSecOps activities into their software development pipelines.
- **There is no universally adopted application security testing (AST) tool.** As the responses to the survey questions indicate, there is no shortage of application security testing tools and techniques. However, even the AST tool with the highest adoption rate is still only utilized by less than half of respondents.
- **The media plays an important role in open source risk management.** Forty-six percent of respondents noted that media coverage had prompted their organization to apply more stringent controls on open source usage.
- **Forty-seven percent of respondents are defining standards around the age of open source components they use** A growing issue in the open source community is project sustainability. A 2020 Synopsys study showed that 91% of codebases audited in 2019 contained open source components that either were more than four years out of date or had no development activity in the past two years. Security risks increase when obsolete code is deployed, including the threat of an open source component being hijacked. Such a situation occurred in 2018 when the event-stream component was hijacked to target Bitcoin in Copay accounts.

To learn more, download a copy of the DevSecOps Practices and Open Source Management in 2020 report.

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle. Learn more at www.synopsys.com/software.

About Synopsys

Synopsys, Inc. (Nasdaq: SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic

products and software applications we rely on every day. As the world's 15th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

Editorial Contact:
Mark Van Elderen
Synopsys, Inc.
650-793-7450
mark.vanelderen@synopsys.com

SOURCE Synopsys, Inc.