Black Duck Newsroom

New Research Finds 73% of Organizations Have Significantly Increased Their Software Supply Chain Security Efforts as a Result of Log4Shell, SolarWinds, and Kaseya

Study conducted by Enterprise Strategy Group highlights the prevalence of software supply chain risks in cloud-native applications

Disclaimer: The Synopsys Software Integrity Group is now Black Duck®. Click here to learn more.

MOUNTAIN VIEW, Calif., Aug. 9, 2022 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today revealed new research based on a recent survey of 350 application development, information technology, and cybersecurity decision-makers. The research, conducted by Enterprise Strategy Group (ESG) and commissioned in part by the Synopsys Software Integrity Group, highlighted within the "Walking the Line: GitOps and Shift Left Security: Scalable, Developer-centric Supply Chain Security Solutions" eBook shows that software supply chain risk extends beyond open source.

In response to software supply chain attacks such as Log4Shell, SolarWinds, and Kaseya, 73% of respondents say they have increased their efforts significantly to secure their organizations' software supply chain through a variety of security initiatives. These initiatives include the adoption of some form of strong multifactor authentication technology (33%), investment in application security testing controls (32%), and improved asset discovery to update their organization's attack surface inventory (30%). Despite those efforts, 34% of organizations report that their applications have been exploited due to a known vulnerability in open source software (OSS) within the last 12 months, with 28% having suffered a previously unknown ("zero-day") exploit found in open source software.

As the scale of OSS usage increases, its presence in applications will naturally increase as well. Current pressure to improve software supply chain risk management has placed a spotlight on software Bills of Materials (SBOMs). But exploding OSS usage and lackluster OSS management has made the compilation of SBOMs complex—as confirmed in the ESG research, which shows that 39% of survey respondents marked this task as a challenge of using OSS.

Download a free copy of the "Walking the Line: GitOps and Shift Left Security: Scalable, Developer-centric Supply Chain Security Solutions" eBook.

"As organizations are witnessing the level of potential impact that a software supply chain security vulnerability or breach can have on their business through high-profile headlines, the prioritization of a proactive security strategy is now a foundational business imperative," said Jason Schmitt, general manager of the Synopsys Software Integrity Group. "While managing open source risk is a critical component of managing software supply chain risk in cloud-native applications, we must also recognize that the risk extends beyond open source components. Infrastructure-as-code, containers, APIs, code repositories—the list goes on and on and must all be accounted for to ensure a holistic approach to software supply chain security."

While open source software may be the original supply chain concern, the shift toward cloud-native application development has organizations concerned about the risks posed to additional nodes of their supply chain. This includes not only additional aspects of source code, but also how cloud-native applications are stored, packaged, and deployed, as well as how they interface with one another through application programming interfaces (APIs). Nearly half (45%) of survey respondents identified APIs as the vector most susceptible to attack, along with data storage repositories (42%) and application container images (34%).

Nearly all (99%) of respondents said their organizations either currently use, or plan to use, OSS within the next 12 months. While concerns exist with the maintenance, security, and trustworthiness of these open source projects, the top concern relates to the scale at which open source is being leveraged within application development. Fifty-four percent of organizations list "having a high percentage of application code that is open source" as their primary concern.

"With the recent US Presidential Executive Order (14028) to improve the nation's cybersecurity, there is significant interest around the importance of a concept known as a software Bill of Materials," said Tim Mackey, principal security strategist within the Synopsys Cybersecurity Research Center. "Effectively, an SBOM allows operators of software to know what third-party software producers included in their applications, whether it be from an open source, commercial or contracted third party. This knowledge is critical when designing a patch management process, as without it there is an incomplete view of the software risks present in any application—regardless of origin. Armed with this information, once the next zero-day vulnerability of Log4Shell proportions emerges (and it will) your organization will be able to act quickly and effectively to defend against attacks targeting third-party software components."

Survey findings also suggest that although developer-focused security and "shifting left"—a concept focused on enabling developers to conduct security testing earlier in the development lifecycle—is growing among organizations building cloud-native applications, 97% of organizations have experienced a security incident involving their cloud-native applications within the last 12 months.

Faster release cycles are also presenting security challenges for all teams. Application development (41%) and DevOps (45%) teams agree that developers often skip established security processes, while a majority of application developers (55%) agree that security teams lack visibility into development processes. Sixty-eight percent of respondents indicated that they are highly prioritizing adopting developer-focused security solutions and shifting some security responsibilities to developers, although more developers (45%) are currently responsible for application security testing than security teams (40%). These developers are twice as likely to use internally developed or open source security tools than specialized third-party vendor solutions.

At the same time, developers are playing a bigger role in securing the software supply chain of cloud-native applications, yet only 36% of security teams reported being comfortable with development teams taking responsibility for testing. Concerns such as overburdening development teams with additional tooling and responsibilities, disrupting innovation and velocity, and obtaining oversight around security efforts remain the biggest obstacles to developer-led application security efforts.

Those interested in learning more about the research can download a complimentary copy of the "Walking the Line: GitOps and Shift Left Security: Scalable, Developer-centric Supply Chain Security Solutions" eBook or read our blog post with more in-depth insights into the survey's findings.

Attendees of the Black Hat USA conference are welcome to visit us at booth #1560 in the expo hall to discuss these findings in more depth.

To learn more about how Synopsys Software Integrity Group is able to minimize security risks while maximizing speed and productivity, visit: www.synopsys.com/software-integrity.html

Press Contact
Liz Samet
Synopsys, Inc.
336-414-6753
esamet@synopsys.com

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 an S&P 500 company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and offers the industry's broadest portfolio of application security testing tools and services. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing more secure, high-quality code, Synopsys has the solutions needed to deliver innovative products. Learn more at www.synopsys.com.

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2022-08-09-New-Research-Finds-73-of-Organizations-Have-Significantly-Increased-Their-Software-Supply-Chain-Security-Efforts-as-a-Result-of-Log4Shell,-SolarWinds,-and-Kaseya