Synopsys Study Highlights Core Challenges with Managing Open Source Risk in Software Supply Chains

Analysis of more than 2,400 commercial and proprietary codebases finds decreases in open source license and vulnerability risks, but 88% of organizations still behind in keeping open source updated

MOUNTAIN VIEW, Calif., April 12, 2022 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the 2022 Open Source Security and Risk Analysis (OSSRA) report. The report, produced by the Synopsys Cybersecurity Research Center (CyRC), examines the results of more than 2,400 audits of commercial and proprietary codebases from merger and acquisition transactions, performed by the Black Duck® Audit Services team. The report highlights trends in open source usage within commercial and proprietary applications and provides insights to help developers better understand the interconnected software ecosystem. It also details the pervasive risks posed by unmanaged open source, including security vulnerabilities, outdated or abandoned components, and license compliance issues.

The 2022 OSSRA report findings underscore the fact that open source is used everywhere, in every industry, and is the foundation of every application built today.

- **Outdated open source remains the norm—including presence of vulnerable Log4j versions.** From an operational risk/maintenance perspective, 85% of the 2,097 codebases contained open source that was more than four years out-of-date. 88% utilized components that were not the latest available version. 5% contained a vulnerable version of Log4j.

- **Assessed codebases show open source vulnerabilities are decreasing overall.** 2,097 of the assessed codebases included security and operational risk assessments. There was a more dramatic decrease in the number of codebases containing high-risk open source vulnerabilities. 49% of this year's audited codebases contained at least one high-risk vulnerability, compared to 60% last year. Additionally, 81% of the assessed codebases contained at least one known open source vulnerability, a minimal decrease of 3% from the findings of the 2021 OSSRA.

- **License conflicts are also decreasing overall.** Over half—53%—of the codebases contained license conflicts, a substantial decrease from the 65% seen in 2020. In general, specific license conflicts decreased across the board between 2020 and 2021.

- **20% of assessed codebases contained open source with no license or with a customized license.** Since a software license governs the right to use it, software with no license presents the dilemma of whether use of the open source component entails legal risk. Additionally, customized open source licenses might place undesirable requirements on the licensee and will often require legal evaluation for possible IP issues or other implications.

"Users of SCA software have focused their attention on reducing open source license issues and addressing high-risk vulnerabilities, and that effort is reflected in the decreases we saw this year in license conflicts and high-risk vulnerabilities, said Tim Mackey, principal security strategist with the Synopsys Cybersecurity Research Center. "The fact remains that over half of the codebases we audited still contained license conflicts and nearly half still contained high-risk vulnerabilities. Even more troubling was that 88% of the codebases [with risk assessments] contained outdated versions of open source components with an available update or patch that was not applied."

"There are justifiable reasons for not keeping software completely up-to-date," Mackey continued. "But, unless an organization keeps an accurate and up-to-date inventory of the open source used in their code, an outdated component can be forgotten until it becomes vulnerable to a high-risk exploit, and then the scramble to identify where it's being used and to update it is on. This is precisely what occurred with Log4j, and why software supply chains and Software Bill of Materials (SBOM) are such hot topics."

To learn more about the potential risks associated with open source software and how to address them, download a copy of the 2022 OSSRA report, read the blog post, or register for the April 28th webinar.

About the Synopsys Software Integrity Group

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that's best for them. Only Synopsys offers everything you need to build trust in your software. 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.

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

SOURCE Synopsys, Inc.