Synopsys Study Shows Uptick in Vulnerable, Outdated, and Abandoned Open Source Components in Commercial Software

Analysis of more than 1,500 commercial codebases finds that open source security, license compliance, and maintenance issues are pervasive in every industry sector

MOUNTAIN VIEW, Calif., April 13, 2021 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the 2021 Open Source Security and Risk Analysis (OSSRA) report. The report, produced by the Synopsys Cybersecurity Research Center (CyRC), examines the results of more than 1,500 audits of commercial codebases, performed by the Black Duck® Audit Services team. The report highlights trends in open source usage within commercial applications and provides insights to help commercial and open source developers better understand the interconnected software ecosystem they are part of. It also details the pervasive risks posed by unmanaged open source, including security vulnerabilities, outdated or abandoned components, and license compliance issues.

The 2021 OSSRA report affirms that open source software provides the foundation for the vast majority of applications across all industries. It also shows that those industries, to varying degrees, are struggling to manage open source risk.

- 100% of the companies audited in the marketing tech industry sector—which includes lead generation CRM, and social media—contained open source in their codebases. 95% of the marketing tech codebases contained open source vulnerabilities.
- 98% of healthcare sector codebases contained open source. 67% of those codebases contained vulnerabilities.
- 97% of financial services/fintech sector codebases contained open source. Over 60% of those codebases contained vulnerabilities.
- 92% of codebases in the retail and e-commerce sector contained open source, and 71% of the codebases in that sector contained vulnerabilities.

Of even more concern is the widespread use of abandoned open source components. An alarming 91% of the codebases contained open source dependencies that had no development activity in the last two years—meaning no code improvements and no security fixes.

"That more than 90% of the codebases were using open source with no development activity in the past two years is not surprising," said Tim Mackey, principal security strategist with the Synopsys Cybersecurity Research Center. "Unlike commercial software, where vendors can push information to their users, open source relies on community engagement to thrive. When an open source component is adopted into a commercial offering without that engagement, project vitality can easily wane. Orphaned projects aren't a new problem, but when they occur, addressing security issues becomes that much harder. The solution is a simple one – invest in supporting those projects you depend upon for your success."

Other open source risk trends identified in the 2021 OSSRA report include:

- **Outdated open source components in commercial software is the norm.** 85% of the codebases contained open source dependencies that were more than four years out-of-date. Unlike abandoned projects, these outdated open source components have active developer communities who publish updates and security patches that are not being applied by their downstream commercial consumers. Beyond the obvious security implications of neglecting to apply patches, the use of outdated open source components can contribute to unwieldy technical debt in the form of functionality and compatibility issues associated with future updates.
- **The prevalence of open source vulnerabilities is trending in the wrong direction.** In 2020, the percentage of codebases containing vulnerable open source components rose to 84%—a 9% increase from 2019. Similarly, the percentage of codebases containing high-risk vulnerabilities jumped from 49% to 60%. Several of the top 10 open source vulnerabilities that were found in codebases in 2019 reappeared in the 2020 audits, all with significant percentage increases.
- **Over 90% of the audited codebases contained open source components with license conflicts, customized licenses, or no license at all.** 65% of the codebases audited in 2020 contained open source software license conflicts, typically involving the GNU General Public License. 26% of the codebases were using open source with no license or a customized license. All three issues often need to be evaluated for potential intellectual property infringement and other legal concerns, especially in the context of merger and acquisition transactions.

To learn more about the potential risks associated with open source software and how to address them, download a copy of the 2021 OSSRA report, read the blog post, or register for the April 21 webinar.

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

SOURCE Synopsys, Inc.