Synopsys Report Finds that Open Source Risk Management is Improving, but Still a Challenge for Most Organizations

Study of more than 1,200 commercial applications and libraries finds a majority still contain open source security vulnerabilities and license conflicts

MOUNTAIN VIEW, Calif., April 30, 2019 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the 2019 Open Source Security and Risk Analysis (OSSRA) report. The report, produced by the Synopsys Cybersecurity Research Center (CyRC), examines the results of more than 1,200 audits of commercial applications and libraries, performed by the Black Duck Audit Services team. The report highlights trends and patterns in open source use, as well as the prevalence of both insecure open source components and license conflicts.

As shown in the report, many of the trends in open source use that have presented risk management challenges to organizations in previous years persist today. However, the data also suggest that an inflection point has been reached, with many organizations improving their ability to manage open source risk, possibly due to heightened awareness and the maturation of commercial software composition analysis solutions.

"Open source plays an increasingly vital role in modern software development and deployment, but to realize its value organizations need to understand and manage how it impacts their risk posture from a security and license compliance perspective," said Tim Mackey, principal security strategist of the Synopsys Cybersecurity Research Center. "The 2019 OSSRA report provides a glimpse into the state of open source risk management within commercial applications. It shows that there are still significant challenges, with the majority of applications containing open source security vulnerabilities and license conflicts. But it also highlights that these challenges can be addressed, as the number open source vulnerabilities and license conflicts have declined from the previous year."

Some of the most noteworthy open source risk trends identified in the 2019 OSSRA report include:

- **There has been a significant uptick in open source adoption.** Ninety-six percent of codebases audited in 2018 contained open source components, with an average of 298 open source components per codebase compared to 257 in 2017.
- **Open source license conflicts can put intellectual property at risk.** Sixty-eight percent of codebases contained some form of open source license conflict, and 38% contained open source components with no identifiable license.
- **The use of 'abandoned' components is common.** Eighty-five percent of codebases contained components that were more than four years out-of-date or had no development in the past two years. If a component is inactive and no one is maintaining it, that means no one is addressing its potential vulnerabilities.
- **Many organizations are failing to patch or update their open source components.** The average age of vulnerabilities identified in 2018 Black Duck Audits was 6.6 years, slightly higher than 2017—suggesting remediation efforts haven't improved significantly. Forty-three percent of the codebases scanned in 2018 contained vulnerabilities over 10 years old. When viewed against the backdrop of the National Vulnerability Database adding over 16,500 new vulnerabilities in 2018, its clear patch processes need to scale to accommodate increased disclosures.
- **Not all vulnerabilities are created equal, but many organizations aren't even addressing the riskiest ones.** Over 40% of codebases contained at least one high-risk open source vulnerability.

The report notes that the use of open source software is not a problem in and of itself, and is, in fact, essential to software innovation. But failing to proactively identify and manage any security and license risks associated with the usage of open source components can be very damaging. Despite the risk factors identified, the 2019 OSSRA data suggests that, in the wake of the Equifax breach, an increase in awareness of open source risk and the maturation of commercial software composition analysis solutions has led to forward progress:

- **Organizations are getting better at managing open source security vulnerabilities.** Sixty percent of the codebases audited in 2018 contained at least one vulnerability—still significant, but much better than the figure of 78% from 2017.
- **Overall, open source license compliance has improved as well.** Sixty-eight percent of the 2018 audited codebases contained components with license conflicts, compared to 74% in 2017.

To learn more, download a copy of the 2019 OSSRA report, or register for our May 9th webinar, 2019 Open Source Security Report: Persistent Challenges and Forward Progress.

About the Synopsys Software Integrity Platform

Synopsys Software Integrity Group helps organizations 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 http://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 Contacts:
Mark Van Elderen
Synopsys, Inc.
650-793-7450
mark.vanelderen@synopsys.com

SOURCE Synopsys, Inc.