Synopsys Report Finds Majority of Software Plagued by Known Vulnerabilities and License Conflicts as Open Source Adoption Soars

The findings show a third of the audited codebases that contained Apache Struts also had the vulnerability that resulted in the Equifax breach

MOUNTAIN VIEW, Calif., May 15, 2018 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the Black Duck by Synopsys 2018 Open Source Security and Risk Analysis (OSSRA) report, which examines findings from the anonymized data of over 1,100 commercial codebases audited in 2017. Industries represented in the report include the automotive, big data, cyber security, enterprise software, financial services, healthcare, Internet of Things (IoT), manufacturing, and mobile app markets.

The report highlights a massive uptick in open source adoption, with 96 percent of the applications scanned containing open source components. The data also shows that the average number of open source components found per codebase (257) grew by 75 percent over the previous year, with many applications containing more open source than proprietary code. What is worrisome is that 78 percent of the codebases examined contained at least one open source vulnerability, with an average 64 vulnerabilities per codebase. Over 54 percent of the vulnerabilities found in audited codebases are considered high-risk vulnerabilities. Seventeen percent of the codebases contained a highly publicized vulnerability such as Heartbleed, Logjam, Freak, Drown, or Poodle.

"Since modern software and infrastructure depend heavily on open source technologies, having a clear view of components in use is a key part of corporate governance," said Tim Mackey, technical evangelist at Black Duck by Synopsys. "The report clearly demonstrates that with the growth in open source use, organizations need to ensure they have the tools to detect vulnerabilities in open source components and manage whatever license compliance their use of open source may require."

Vulnerable open source components were found in applications in every industry. The Internet and Software Infrastructure vertical had the highest proportion—67 percent—of applications containing high-risk open source vulnerabilities. Ironically, 41 percent of the applications in the Cyber Security industry were found to have high-risk open source vulnerabilities, putting that vertical at fourth highest risk.

In addition, 33 percent of the audited codebases that contained Apache Struts also contained the vulnerability that resulted in the Equifax breach. The report clearly shows that organizations are allowing a growing number of vulnerabilities to accumulate in their codebases. On average, vulnerabilities identified in the audits were disclosed nearly six years ago.

"When Equifax was breached through the Apache Struts vulnerability, the need for open source security management became front-page news," said Evan Klein, the Black Duck product marketing manager responsible for the OSSRA report. "Yet even though it was disclosed in March 2017, many organizations apparently still have not checked their applications for the Struts vulnerability."

Based on the findings, 74 percent of the codebases audited also contained components with license conflicts, the most common of which were GPL license violations. The percentage of applications with license conflicts within verticals ranged from the Retail and E-commerce industry's relative low of 61 percent to the high of the Telecommunications and Wireless industry—where 100 percent of the code scanned had some form of open source license conflict.

To download the OSSRA report, visit https://www.blackducksoftware.com/open-source-security-risk-analysis-2018.

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

Simone Souza
Synopsys, Inc.
650-584-6454
simone@synopsys.com

SOURCE Synopsys, Inc.