Synopsys Research Highlights the Pervasive Use of Outdated and Insecure Third-Party Software Components

Analysis of More Than 120,000 Applications Found that Half of Third-Party Software Components in Use Are Outdated

MOUNTAIN VIEW, Calif., June 6, 2017 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released its report, "The State of Software Composition 2017," which analyzed real-world data to investigate the security of the software supply chain one of the most significant challenges the software industry faces today. The report summarizes the analysis of 128,782 software applications, which identified 16,868 unique versions of open source and commercial software components containing almost 10,000 unique security vulnerabilities.

Synopsys used its software composition analysis product, Protecode™ SC, to analyze applications scanned from January 1, 2016 through December 31, 2016. Of the 3rd party software components identified through the analysis of these applications, nearly 50 percent of these components were more than four years old, and in almost every case a newer, more secure version of the software component is available.

"By analyzing large data sets and identifying trends and problem areas, we are able to provide the software development community with valuable intelligence to help them keep their software secure and up to date," said Andreas Kuehlmann, senior vice president and general manager for the Synopsys Software Integrity Group. "Over time, vulnerabilities in third-party components are discovered and disclosed, leaving a previously secure software package open to exploits. The message to the software industry should not be whether to use open source software, but whether you are vigilant about keeping it updated to prevent attacks."

The research, upon which the report is based, represents a cross section of software including mobile, desktop and web applications, as well as firmware and embedded software from a variety of industries. The report includes information on the most commonly observed 3rd party software components, the Common Vulnerabilities and Exposures (CVE) known to affect these components, the 10-point Common Vulnerability Scoring System (CVSS) rank for CVE and the Common Software Weaknesses (CWE) used to classify them.

Other key findings include:

- 45 percent of the total 9,553-specific CVEs date back to 2013 or earlier
- The Heartbleed bug still appears in the top 50 percent of all CVEs observed, even though a patch has been available since 2014
- The oldest CVE dates back to 1999
- The top 10 most common software components with outdated versions still being used more than 90 percent of the time include: Curl, Dropbear, Expat, libjpeg-turbo, libjpeg, libpng Linux Kernal, Lua, OpenSSL, and Pcre; if they are not updated, these software components may leave products vulnerable

"Coming on the heels of last month's WannaCry outbreak, the insights in the report serve as a wakeup call that not everyone is using the most secure version of available software," said Robert Vamosi, security strategist at Synopsys. "The update process does not end at the time of software release, and an ongoing pattern of software updates must be implemented throughout the product lifecycle. As new CVEs are disclosed against open source software components, developers need to know whether their products are affected, and organizations need to prevent the exploit of vulnerabilities with the latest versions when they become available."

Download the full report here.

About the Synopsys Software Integrity Platform

Through its Software Integrity Platform, Synopsys provides advanced solutions and services for improving software security and quality. This comprehensive platform of automated analysis and testing technologies integrates seamlessly into the software development process and enables organizations to detect and remediate quality defects, security vulnerabilities and compliance issues early in the software development lifecycle, as well as to gain security assurance and visibility into their software supply chain. Learn more at www.synopsys.com/software-integrity.

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

SOURCE Synopsys, Inc.