Black Duck Newsroom

Synopsys 2017 Coverity Scan Report Finds Significant Adoption of Secure Practices in OSS Projects

Report highlights progress over past decade, identifying key indicators of project maturity and underscoring the importance of measuring risk

Disclaimer: The Synopsys Software Integrity Group is now Black Duck®. Click here to learn more.

MOUNTAIN VIEW, Calif., Oct. 31, 2017 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today released the 2017 Coverity® Scan Report, which examines Open Source Software (OSS) quality and security data collected over the past decade through Coverity Scan, a free static analysis solution from Synopsys used by more than 4,600 active OSS projects. The report finds significant adoption of secure software development practices and underscores the importance of managing OSS risk. In addition, it highlights the contributions Coverity Scan has made to the quality of OSS development practices and the overall maturity of the OSS ecosystem. Read the complete report.

"Due to the ubiquity of open source and the vital role it plays in virtually all types of software, understanding and managing its risks can no longer be optional," said Andreas Kuehlmann, senior vice president and general manager of the Synopsys Software Integrity Group. "The Coverity Scan Report highlights the progress of some of the most mature and widely used open source projects, and it provides invaluable insights for the broader software community that depends on the integrity of open source."

Since its inception in 2006, Coverity Scan identified more than 1.1 million defects in active OSS projects, leading to the remediation of more than 600,000 defects. The 2017 Coverity Scan report details the analysis of approximately 760 million lines of open source code across several languages, including C/C++, C#, Java, JavaScript, Ruby, PHP, and Python.

Key findings from the Coverity Scan Report:

- **Active projects within Scan show significant adoption of secure software development practices.** Since January 2016, 4,117 active projects have submitted builds for analysis. Of those, nearly 50 percent (2,049) use Travis CI, indicating using of continuous integration/continuous deployment (CI/CD) practices. Other 2,509 projects have been triaged, which require developers to have intimate knowledge of the codebase. Additionally, 1,120 projects were configured to make use of modeling, a mechanism for improving the quality of their analysis results.
- **Key behaviors indicate increasing maturity of OSS projects.** The adoption of CI/CD and remediation of actionable defects by developers highlight the value of static analysis to the OSS ecosystem. Other measures of maturity such as development and community metrics are required to characterize the risks associated with OSS consumption.
- **Commercial and OSS ecosystems are converging.** According to some of the largest commercial users of Coverity, software shipped to customers can contain up to 90 percent open source code. In addition, there are now companies founded entirely on OSS proving that OSS is now the norm.

Synopsys Coverity Scan helps reduce risk and lower overall project cost by identifying critical quality defects and potential security vulnerabilities during the software development. Synopsys manages the Coverity Scan project and provides Static Application Security Testing (SAST) as a free service to the open source community to help them build quality and security into their software lifecycle. Read more about Coverity Scan.

On November 8, at 12 p.m. PT, Synopsys will be hosting on its community a live discussion on the results of 2017 Coverity Scan Report. Sign up.

About the Synopsys Software Integrity Platform

Synopsys offers the most comprehensive solution for building integrity—security and quality—into the software development lifecycle and supply chain. The Software Integrity Platform unites leading testing technologies, automated analysis, and experts to create a robust portfolio of products and services. This portfolio enables companies to develop personalized programs for detecting and remediating defects and vulnerabilities early in the development process, minimizing risk and maximizing productivity. Synopsys, a recognized leader in application security testing, is uniquely positioned to adapt and apply best practices to new technologies and trends such as IoT, DevOps, CI/CD, and the Cloud. For more information, go to 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:

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

SOURCE Synopsys, Inc.

---

https://news.blackduck.com/2017-10-31-Synopsys-2017-Coverity-Scan-Report-Finds-Significant-Adoption-of-Secure-Practices-in-OSS-Projects