Black Duck Newsroom

Synopsys Expands Coverity Support for New Programming Languages, Secure Coding Standards, and DevOps Toolchain Integrations

Latest release adds support for Scala and VB.NET, SEI CERT C Coding Standard, and enhanced Jenkins plugin

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

MOUNTAIN VIEW, Calif., Jan. 30, 2018 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today announced its Coverity® 2018.01 release, the newest version of its industry-leading static analysis tool, which analyzes source code to detect critical quality and security defects early in the software development life cycle. Coverity 2018.01 extends the tool's support for new programming languages, coding standards, and development tool integrations.

Coverity 2018.01 highlights:

- Introduces support for Scala and VB.NET
- Provides full support for SEI CERT C coding standard rules (2016 edition)
- Includes enhanced plugins for Jenkins continuous integration (CI) server to enable automated testing in DevOps environments

"Secure, high quality software is becoming increasingly an imperative for business success and the well-being of end users in the face of the growing threat landscape," said Andreas Kuehlmann, general manager of the Synopsys Software Integrity Group. "In parallel, the pace and process by which software is developed are changing dramatically. For this reason, the tools used to find defects and potential security vulnerabilities throughout the development life cycle need to evolve as well. By supporting new programming languages, secure coding standards, and out-of-the-box integrations with modern development tools, Synopsys enables organizations to expand their software portfolios and embrace new development paradigms like DevOps with the assurance that their code is high quality and secure."

Coverity has been recognized as a leading application security testing solution by Gartner, Forrester, IDC, and VDC, and is a core component of the Synopsys Software Integrity Platform. The new enhancements and features of Coverity 2018.01 include these:

- **Expanded language coverage**: Coverity enables organizations to proactively build security and quality into their applications, even as they broaden their software portfolios and embrace new languages, frameworks, and technologies such as mobile and microservices. With each release, Synopsys continues to expand Coverity's support for new programming languages while strengthening its security analysis for existing languages. Coverity 2018.01 adds support for two new languages: Scala, commonly used in microservices-based application development, and VB.NET. The latest Coverity release also provides enhanced security analysis for Swift, PHP, Python, JavaScript, Java, C#, and Node.js. With these additions, Coverity supports the key programming languages used to build embedded and enterprise software.
- **Support for secure coding standards**: Coverity enables organizations to comply with coding standards that promote the security, reliability, and safety of critical embedded software. With the latest 2018.01

release, Coverity fully supports SEI CERT C (2016 edition), an industry standard for secure coding. In addition to CERT C, Coverity also supports all versions of the MISRA coding standard and is ISO 26262 certified.

- **Integration with modern development toolchains**: Coverity is designed to support rapid and automated development workflows, with support for and integration with many of the popular development tools. Coverity 2018.01 provides plugins for the latest IDEs, including Visual Studio, Eclipse, IntelliJ, Android Studio, and many others. For streamlined security testing, the latest release also supports out-of-the-box integration with Jenkins continuous integration (CI) server. Coverity's new Jenkins plugin has improved Jenkins Pipeline support, which enables retrieval of found issues by project and has enhanced data-filtering capabilities.

Learn more about Coverity Static Analysis.

About the Synopsys Software Integrity Platform

Synopsys offers the most comprehensive solution for building integrity—security and quality—into the software development life cycle 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 (AST), 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:
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.

https://news.blackduck.com/2018-01-30-Synopsys-Expands-Coverity-Support-for-New-Programming-Languages-Secure-Coding-Standards-and-DevOps-Toolchain-Integrations