Black Duck Newsroom

Coverity Scan Open Source Report Shows Commercial Code Is More Compliant to Security Standards than Open Source Code

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

MOUNTAIN VIEW, Calif., July 29, 2015 /PRNewswire/ -- Synopsys, Inc. (Nasdaq: SNPS) today announced the release of its annual Coverity Scan® Open Source Report. The 2014 report details the analysis of nearly 10 billion lines of source code through the Coverity Scan service and commercial usage of the Synopsys Coverity® Software Testing Platform, the largest sample size that the report has studied to date. For the report, the company analyzed code from more than 2,500 open source C/C++ projects as well as an anonymous sample of commercial projects in 2014. Additionally, the report highlights results from several popular, open source Java and C# projects that have joined the Coverity Scan service since March 2013.

The Coverity Scan Open Source Report has become a widely accepted standard for measuring the state of open source code quality. Since its inception nine years ago, the Coverity Scan service has analyzed billions of lines of code, and as of today has reviewed more than 5,100 open source projects – including C/C++ projects such as Linux, FreeBSD, LibreOffice, Python, PostgreSQL, Firefox and NetBSD, and Java projects such as Apache Hadoop, HBase, Tomcat, Cloudstack and Cassandra. The Coverity Scan service has helped developers find and fix more than 240,000 defects since 2006. As detailed in the new Coverity Scan Open Source Report, nearly 152,000 defects were fixed in 2014 alone – more than the total amount of defects that had been found in the previous history of the service.

Based on static analysis defect density, open source code outpaced commercial code for quality in the 2013 report. This trend continues in 2014; however, this year the report also compared security compliance standards such as OWASP (Open Web Application Security Project) Top 10 and CWE (Common Weakness Enumeration) 25, and found that commercial code is more compliant with these standards than open source code.

Key findings from the latest report include:

- **Defect density** (**defects per 1,000 lines of code) of open source code and commercial code has continued to improve since 2013:** When comparing overall defect density numbers between 2013 and 2014, the defect density of both open source code and commercial code has continued to improve. Open source code defect density improved from 0.66 in 2013 to 0.61 in 2014, while commercial code defect density improved from 0.77 to 0.76.
- **Coverity Scan aids OpenSSL in post-Heartbleed investigation:** According to OpenSSL co-founder Tim Hudson, the Coverity Scan service helped to catch newly discovered defects and highlight where other issues like the Heartbleed bug might exist. Since Heartbleed, OpenSSL has fixed 302 defects found by Coverity Scan, and now has a 0.21 defect density.
- **Linux remains a benchmark for static analysis defect density:** Since joining the Coverity Scan service in 2006, Linux has retained its commitment to quality, which remains a key focus. During 2014, Linux leveraged the Coverity Scan service to find and fix more than 500 high-impact defects, including resource leaks, memory corruptions and uninitialized variables.

"As a whole, software quality and security are improving, but neither open source nor commercial standards are

complete or conclusive enough to catch everything," said Zack Samocha, director of marketing for the Software Integrity Group at Synopsys. "As software projects are being pushed to market faster than ever before, developers need to balance security with speed. As more of these projects use solutions like Coverity Scan, we expect to see continued improvement in open source and commercial code security throughout 2015."

Online Resources

- Download a full copy of the 2014 Coverity Scan Report
- Read our Development Testing blog
- Register your C/C++, Java or C# open source project for the Coverity Scan service

About Coverity Scan

In 2006, the Coverity Scan service was initiated with the U.S. Department of Homeland Security as a public-private sector research project, focused on open source software quality and security. With the acquisition of Coverity by Synopsys in 2014, Synopsys now manages the project and provides its development testing technology as a free service to the open source community to help them build quality and security into their software development process. To receive the latest updates, register your open source project for the Coverity Scan service and follow us on Twitter.

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 a leader in software quality and security testing with its Coverity® solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest quality and security, Synopsys has the solutions needed to deliver innovative, high-quality, secure products.

Editorial Contact:
Yvette Huygen
Synopsys, Inc.
650-584-4547
yvetteh@synopsys.com

Investor Contact:
Lisa Ewbank
Synopsys, Inc.
650-584-1901

SOURCE Synopsys, Inc.

https://news.blackduck.com/2015-07-29-Coverity-Scan-Open-Source-Report-Shows-Commercial-Code-Is-More-Compliant-to-Security-Standards-than-Open-Source-Code