Coverity Scan Report Finds Open Source Software Quality Outpaces Proprietary Code for the First Time

Coverity Opens Up Access to Free Development Testing Service, Allows Anyone Interested in Open Source Software Quality to View Projects

MOUNTAIN VIEW, Calif., April 15, 2014 /PRNewswire/ -- Coverity, Inc., a Synopsys company (Nasdaq: SNPS), today released the 2013 Coverity Scan™ Open Source Report. The report details the analysis of 750 million lines of open source software code through the Coverity Scan service and commercial usage of the Coverity® Development Testing Platform, the largest sample size that the report has studied to date. For the 2013 Coverity Scan Report, the company analyzed code from more than 700 open source C/C++ projects as well as an anonymous sample of enterprise projects. In addition, the report highlights analysis results from several popular, open source Java projects that have joined the Scan service since March 2013.

The Coverity Scan Open Source Report has become a widely accepted standard for measuring the state of open source quality. During the past eight years, the Coverity Scan service has analyzed several hundreds of millions of lines of code from more than 1,500 open source projects – including C/C++ projects such as NetBSD, FreeBSD, LibreOffice and Linux, and Java projects such as Apache Hadoop, HBase and Cassandra. The Scan service has helped developers find and fix more than 94,000 defects since 2006. Nearly 50,000 defects were fixed in 2013 alone – the largest single number of defects fixed in a single year by Scan users. More than 11,000 of these defects were fixed by the four largest projects in the service: NetBSD, FreeBSD, LibreOffice and Linux.

Key findings in the 2013 report include:

- **Open source code quality surpasses proprietary code quality in C/C++ projects.** Defect density (defects per 1,000 lines of software code) is a commonly used measurement for software quality, and a defect density of 1.0 is considered the accepted industry standard for good quality software. Coverity's analysis found an average defect density of .59 for open source C/C++ projects that leverage the Scan service, compared to an average defect density of .72 for proprietary C/C++ code developed for enterprise projects. In 2013, code quality of open source projects using the Scan service surpassed that of proprietary projects at all code base sizes, which further highlights the open source community's strong commitment to development testing.
- **Linux continues to be a benchmark for open source quality.** By leveraging the Scan service, Linux has reduced the average time to fix a newly detected defect from 122 days to just 6 days. Since the original Coverity Scan Report in 2008, scanned versions of Linux have consistently achieved a defect density of less than 1.0. In 2013, Coverity scanned more than 8.5 million lines of Linux code and found a defect density of .61.
- **C/C++ developers fixed more high-impact defects.** The Coverity analysis found that developers contributing to open source Java projects are not fixing as many high-impact defects as developers contributing to open source C/C++ projects. Java project developers participating in the Scan service only fixed 13 percent of the identified resource leaks, whereas participating C/C++ developers fixed 46 percent. This could be caused in part by a false sense of security within the Java programming community, due to protections built into the language, such as garbage collection. However, garbage collection can be unpredictable and cannot address system resources so these projects are at risk.
- **HBase serves as benchmark for Java projects.** Coverity analyzed more than 8 million lines of code from 100 open source Java projects, including popular Big Data projects Apache Hadoop 2.3 (320,000 lines of code), Apache HBase (487,000 lines of code) and Apache Cassandra (345,000 lines of code). Since joining the Scan service in August 2013, Apache HBase – which is Hadoop's database – fixed more than 220 defects, including a much higher percentage of resource leaks compared to other Java projects in the Scan service (i.e., 66 percent for HBase compared to 13 percent on average for other projects).

"If software is eating the world, then open source software is leading the charge," saidZack Samocha, senior director of products for Coverity. "Our objective with the Coverity Scan service is to help the open source community create high-quality software. Based on the results of this report – as well as the increasing popularity of the service – open source software projects that leverage development testing continue to increase the quality of their software, such that they have raised the bar for the entire industry."

Coverity also announced today that it has opened up access to the Coverity Scan service, allowing anyone interested in open source software to view the progress of participating projects. Individuals can now become Project Observers, which enables them to track the state of relevant open source projects in the Scan service and view high-level data including the count of outstanding defects, fixed defects and defect density.

"We've seen an exponential increase in the number of people who have asked to join the Coverity Scan service, simply to monitor the defects being found and fixed. In many cases, these people work for large enterprise organizations that utilize open

source software within their commercial projects," added Samocha. "By opening up the Scan service to these individuals, we are now enabling a new level of visibility into the code quality of the open source projects, which they are including in their software supply chain."

Online Resources

- Download a full copy of the 2013 Coverity Scan Report
- Read our Development Testing blog
- Register your C/C++ or Java open source project for the Coverity Scan service
- Sign up for our webcast: Best Practices in Open Source Quality

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. Coverity now manages the project, providing 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. Register your open source project for the Coverity Scan service, and follow us on Twitter to get the latest updates.

About Coverity
Coverity, Inc., a Synopsys company (Nasdaq: SNPS), is a leading provider of software quality and security testing solutions. Coverity's award-winning development testing platform helps developers create and deliver better software, faster, by automatically testing source code for software defects that could lead to product crashes, unexpected behavior, security breaches or catastrophic system failure. The world's largest brands rely on Coverity to help ensure the quality, safety and security of their products and services. For more information, visit www.coverity.com, follow us on Twitter or check out our blog.

SOURCE Coverity, Inc.

For further information: Julie Seymour, Coverity, +1.415.321.5230, jseymour@coverity.com; Michelle Kincaid, LEWIS PR for Coverity, +1.415.432.2467, coverity@lewispr.com