Coverity Releases Security Spotlight Report on Critical Security Defects in Open Source Projects

OWASP and C# Capabilities in Coverity Scan Expanded to Support Open Source Community

MOUNTAIN VIEW, Calif., Oct. 15, 2014 /PRNewswire/ -- Coverity, Inc., a Synopsys company (Nasdaq:SNPS), today announced the release of its latest Coverity Scan™ Project Spotlight, which analyzed the security defects detected by its open source software scanning service. In conjunction with the release of the report, Coverity also announced that it would enhance the Coverity Scan service by including the Coverity® Security Advisor solution to the service so projects can now find critical Open Web Application Security Project (OWASP) Top 10 issues. The service has also been expanded to now include C# open source projects.

Recent high-profile vulnerabilities in open source code, including Shellshock, the OpenSSL Heartbleed and GoToFail vulnerabilities, have highlighted the importance of code quality and security for organizations. The Coverity Scan Security Spotlight identifies several common defects and exposures (CVEs) in open source code, and identifies that the GoToFail vulnerability could have been detected in Scan.

Since the inception of the Coverity Scan service in 2006, Coverity has enabled open source projects to find and fix critical security issues, including buffer overflows, integer overflows, and format string errors in C/C++ code. With today's announcement, the company is now enabling Java developers to find and fix security issues in their software code, including all of the OWASP Top 10 and other web application security issues.

The OWASP Top 10 presents the most critical threat to open source code. In the short time since Coverity Scan has been able to detect web application security defects in Java, the service has identified 688 OWASP Top 10 issues in 37 open source projects, including big data, network management, and blog server projects. The following are the specific number of OWASP Top 10 issues found:

Item	Description	Number of Issues Found
A1	Injection	135
A2	Broken Authentication and Session Management	43
A3	Cross-site Scripting (XSS)	139
A4	Insecure Direct Object References	210
A5	Security Misconfiguration	10
A6	Sensitive Data Exposure	8
A7	Missing Function Level Access Control	4
A8	Cross-Site Request Forgery (CSRF)	139
A9	Using Components with Known Vulnerabilities	NA
A10	Unvalidated Redirects and Forwards	0

"The road to application quality and security starts in development," said Zack Samocha, senior director of products at Coverity. "With three major security issues related to open source code defects this year, it's imperative that open source developers design code security into their projects starting as early as possible and utilize security experts to help them understand vulnerable areas in the code and potential attack vectors. Open source developers should leverage some of the best practices for application security employed by proprietary projects such as using static analysis and conducting regular security audits."

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.

Online Resources:

- Download the Coverity Scan Security Spotlight
- Download a full copy of the 2013 Coverity Scan Report
- Read our Development Testing blog

- Join our webcast "Securing Against CSRF in a Way You Won't Regret Later"
- Register your C/C++ or Java 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. 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: Kristin Brennan, Coverity, +1.415.321.5230, kbrennan@coverity.com; or Michelle Kincaid, LEWIS PR for Coverity, +1.415.432.2467, coverity@lewispr.com