

FOR IMMEDIATE RELEASE

**Open Source Software Continually Improving According to
Research from Coverity™ Joint Venture with
U.S. Department of Homeland Security**

*New Scan Report on Open Source Software 2008 Shows 16% Reduction in Static
Analysis Defect Density Across 250 Popular Open Source Projects Over 2 Year Period*

*Researchers Uncover New Information Regarding Defect Density,
Code Base Size and Other Indices of Code Complexity*

SAN FRANCISCO – May 20, 2008 – Coverity™, Inc., the leader in improving software quality and security, today announced the availability of the Scan Report on Open Source Software 2008. The Coverity Scan site was developed with support from the U.S. Department of Homeland Security as part of the federal government's 'Open Source Hardening Project.' The report is based on 2 years of analysis of more than 55 million lines of code on a recurring basis from over 250 popular open source projects with Coverity Prevent™, the industry-leading static source code analysis solution.

"The continued improvement of projects that already possess strong code quality and security underscores the commitment of open source developers to create software of the highest integrity," said David Maxwell, open source strategist for Coverity. "Working with the open source community over the past two years has been an exceptional opportunity for researchers at both the Scan site and Coverity. Based on preliminary feedback from preview readers, the report contains thought provoking information about defect density and code complexity and provides a strong foundation for future research on the nature of software."

Open source projects analyzed at the Scan site include some of the worlds most widely used applications, including the Apache web server and the Linux operating system. Source code analysis from the Scan site is freely available to qualified open source projects at: <http://scan.coverity.com>

"Close collaboration between Coverity and the FreeBSD Project over three years has been both exciting and remarkably valuable," said Robert Watson, FreeBSD foundation president. "Coverity has had a positive impact on the correctness of our source code and has helped improve our software development methodology."

The breadth and volume of analysis data presented in the Scan Report on Open Source Software 2008 is unlike any other collection of code analysis data in existence, representing 14,238 individual project analysis runs for a total of nearly 10 billion lines of code analyzed over 2 years.

The report also draws conclusions that may apply equally to open source and commercial software regarding the relationship between variables such as code base size, defect density, function length, Cyclomatic complexity and Halstead effort. In summary, the Scan Report on Open Source Software 2008 contains the following findings:

- The quality and security of open source software is improving – Researchers at the Scan site observed a 16% reduction in static analysis defect density over the last 2 years, which reflects the elimination of more than 8,500 individual defects
- Prevalence of specific defect types – The report shows a clear distinction between the frequencies of defect types across the scan database. ‘NULL pointer dereference’ was the most common defect while ‘Use before test of negative values’ was the least common defect
- Average project function length and static analysis defect density – Data in the report contradicts conventional wisdom, indicating that projects with large average function length are not prone to higher defect densities
- Cyclomatic complexity and Halstead effort – Research indicates these two measures of code complexity are significantly correlated to code base size
- False positive results – The average rate of false positives identified by open source developers on the Scan site is below 14%

Detailed data and analysis of these and other findings are available in the complete Scan Report on Open Source Software 2008, which is freely available for download in the research library at www.coverity.com

“The use of open-source technologies to enhance and evolve commercial products has become a common strategy. Vendors will continue to leverage this movement by embedding open source into products, while end-user organizations will use stable open-source projects as a competitive differentiator against companies that refuse to acknowledge that open source is now enterprise-ready. By 2012, 80% or more of all commercial software will include elements of open-source technology,” according to analyst Mark Driver in his recent Gartner report ‘Open Source in Vendor Business Strategies, 2008,’ published March 31, 2008.

Results of the Scan Report on Open Source Software 2008 will also be discussed during a complimentary webinar on Wednesday, May 21, 2008 by David Maxwell, Coverity’s open source strategist. Registration is available at: <http://w.on24.com/r.htm?e=107874&s=1&k=41E3686F9B655D193F894D4A844EBBC6>

About the Scan site

The Scan site was developed by Coverity with support from the U.S. Department of Homeland Security as part of the federal government’s ‘Open Source Code Hardening Project’. The site divides open source projects into rungs based on the progress each project makes in resolving defects. Projects at higher rungs receive access to additional analysis capabilities and configuration options. Projects are promoted as they resolve the majority of defects identified at their current rung.

About Coverity

Coverity (www.coverity.com), the leader in improving software quality and security, is a privately held company headquartered in San Francisco. Coverity's groundbreaking technology enables developers to control complexity in the development process by automatically finding and helping to repair critical software defects and security vulnerabilities throughout the application lifecycle. More than 450 leading companies including ARM, Phillips, RIM, Rockwell-Collins, Samsung and UBS rely on Coverity to help them ensure the delivery of superior software.

###

Coverity is a registered trademark, and Coverity Extend and Coverity Prevent are trademarks of Coverity, Inc. All other company and product names are the property of their respective owners.

Media Contacts

Jim Shissler
Director, Public Relations
jshissler@coverity.com
+1 415 694 5342

Steve Eisenstadt
Page One Public Relations
steve@pageonepr.com
+1 (919) 781-8096