Veracode State of Software Security Report Uncovers Significant Weaknesses in Security Vendor Applications

Submitted by: Hothouse Communications
Tuesday, 19 April 2011

Veracode State of Software Security Report Uncovers Significant Weaknesses in Security Vendor Applications

Research Shows a Slight Decline in the Percentage of SQL Injection Errors Across All Industry Applications, While Prevalence of Cross-Site Scripting Errors Remains Unchanged

LONDON – Infosecurity Europe 2011 (Booth #B90) – April 19, 2011 – With the trend of targeted cyber attacks along with the exploitation of common vulnerabilities such as SQL Injection, it is clear that the core software infrastructure of several critical industries remains extremely vulnerable. Released today, the Veracode "State of Software Security Report: Volume 3" uncovered that those security vendors tasked with protecting enterprises are often the most at risk due to the poor quality of their very own software applications. In fact, 72 percent of security products and services applications analyzed in this report failed to meet acceptable levels of security quality.

In its most recent State of Software Security report, Veracode analyzed 4,835 applications that were submitted to its cloud-based application security testing platform for independent security verification. That number is nearly double from the previous report (September 2010) and represents applications analyzed over the past 18 months. Despite many new findings, there is one constant data point: software remains fundamentally flawed. In fact, 58 percent of all software applications across supplier types continued to fail to meet acceptable levels of security quality upon initial submission to Veracode's service.

What's New: From Software Industry Risks to SQL Injection Trends
Volume 3 includes several new areas of analysis including a deep dive on the software industry, quarterly trending information on the prevalence of common vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS) errors, a study of flaw remediation behavior, and software developer education and training statistics.

What makes this data especially valuable is that compared to reports that extrapolate findings after an attack, Veracode examines unknown application vulnerabilities prior to a breach, and often prior to deployment, to identify where potential weaknesses exist. Specific highlights include:

• 66 percent of software industry applications were found to be of unacceptable security quality upon initial submission, a clear sign that significant work needs to be done just to equal the 58 percent unacceptable rate for applications across all industries.

• 72 percent of security products and services applications had unacceptable security quality: The two worst performers within the software industry upon initial submission were the categories of customer support, such as CRM and web customer support applications (82 percent unacceptable), followed by security products and services (72 percent unacceptable).

• Private versus public software vendor applications – little discernable difference: Despite the heightened scrutiny faced by public companies and perhaps elevated expectations for application security, Veracode found little discernable differences in terms of security quality between the two sectors.

• Even with its flaws, the software industry moves swiftly to remediate errors: Overall, more than 90 percent of all applications across the software industry achieved acceptable security policy within 30 days. The average for all applications in the security products and services sub-category was an impressive three days. This data illustrates how easy it is to fix a flaw once it has been identified.

• SQL Injection errors slowly declining: Despite elevated awareness and frequency of exploitation in high-profile attacks, the percentage of applications infected with SQL Injection errors declined only slightly, 2.4 percent per quarter over the past eight quarters. The prevalence of XSS errors remaining largely unchanged.

“While somewhat surprising, our findings related to the quality of security product and services vendors seem to corroborate recent headlines associated with the high-profile, but not especially sophisticated attacks, on prominent security vendors such as HBGary, Comodo, Barracuda Networks and EMC’s RSA division. These findings should reinforce that no industry sector is immune to application security risk,” said Matt Moynahan, CEO, Veracode, Inc. “Our goal with these State of Software Security reports is to continue to raise awareness of the prominence of common vulnerabilities, such as those caused by SQL Injection or XSS errors, while providing organizations with confidence that with the right training, tools and C-level commitment, that high-quality software is possible, without a tremendous time investment.”

Emphasizing the Case for Third-Party Software Validation

The Epsilon breach served as a spectacular reminder about security risks for organizations that rely on third-party software to run core business functions. According to the Veracode report, Finance and Software & IT Services lead the charge for independent third-party risk assessments and software supplier accountability. Together, these industry segments represented more than 75 percent of the enterprises requesting formal verification of third-party suppliers. Additionally, the report showed that the Aerospace and Defense industry followed suit with its own efforts to apply new rigor to securing its software supply chain.

Reliance on third-party software will only increase with the adoption of cloud and mobile platforms. As such, CIOs and CISOs, particularly in the Finance, Software & IT Services, and Aerospace and Defense industries, should follow their peers’ efforts to protect their infrastructure against the dangers of insecure software.

Building or Requiring Secure Software Doesn’t Have to Be Time Consuming

Veracode understands the inherent concern among developer and security teams about gaining organizational buy-in for undertaking regular testing and programs. However, new data from this report seeks to debunk the assumption that remediation is simply too time intensive of a process to undertake.

More than 50 percent of commercial suppliers in Veracode’s data set resubmitted 90-100 percent of their applications. Slightly under 40 percent of companies developing applications internally resubmitted

90-100 percent of their applications. When all applications were measured against Veracode's risk adjusted verification methodology, more than 80 percent of applications across all supplier types achieved an acceptable security rating within 30 days.

Making the Case for Application Security Training

While seemingly common sense that better developer training would lead to higher quality applications, Veracode is one of the first companies to link the prevalence of insecure software with quantifiable gaps in security competency and understanding. In analyzing data associated with its eLearning program participants, Veracode found that more than 50 percent of those who took an application security fundamentals exam received a grade of C or lower. More than 30 percent received a failing grade of D or F. This data supports the critical need for organizations to take responsibility for instituting more rigorous, contextual developer training and education programs to improve application security competency levels.

Access to Report and Webinar Details

To learn more, download the complete State of Software Security Report: Volume 3 by visiting: http://info.veracode.com/state-of-software-security-report-volume3.html. Veracode will also present the findings in webinars taking place Wednesday, April 20. Attendees can choose from an 11 a.m. ET or 2 p.m. ET presentation. To register, please visit http://www.veracode.com/events/index.html.

About Veracode

Veracode is the only independent provider of cloud-based application intelligence and security verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. By combining patented static, dynamic and manual testing, extensive eLearning capabilities, and advanced application analytics Veracode enables scalable, policy-driven application risk management programs that help identify and eradicate numerous vulnerabilities by leveraging best-in-class technologies from vulnerability scanning to penetration testing and static code analysis. Veracode delivers unbiased proof of application security to stakeholders across the software supply chain while supporting independent audit and compliance requirements for all applications no matter how they are deployed, via the web, mobile or in the cloud. Veracode works with customers in more than 80 countries worldwide including Global 2000 brands such as Barclays PLC and Computershare as well as the California Public Employees' Retirement System (CalPERS) and the Federal Aviation Administration (FAA). For more information, visit www.veracode.com, follow on Twitter: @Veracode or read the ZeroDay Labs blog.

# # #

Media Contacts:
Liz Campbell (for Veracode U.S.)
fama PR
phone: +1 617-986-5009

email: veracode@famapr.com

Paula Averley (for Veracode UK)
Hothouse Communications
phone: (44) (0)20 8224 9933
mobile: (44) 7766 257776
email: veracode@hothousecomms.com