Veracode Study of Software Related Cybersecurity Risks in Public Companies Finds that Majority of Applications Are A Risk

Submitted by: Origin Comms Ltd
Tuesday, 24 April 2012

Despite Higher Compliance Requirements, Public Companies Fare No Better Than Companies At Large On Software Security

LONDON, UK – April 24, 2012 – Veracode, Inc., the leader in cloud-based application security testing, today released a feature supplement of its annual “State of Software Security Report” which showed that 84 percent of web applications from public companies were deemed unacceptable when measured against the OWASP Top 10, a widely used industry standard list of critical and most frequently exploited web application vulnerabilities.

Non-web applications such as backend operational systems and desktop commercial applications in use at public companies also showed a poor performance with a 63 percent failure rate when measured against the CWE/SANS Top 25 – an industry standard list of critical non-web application vulnerabilities.

Unlike previous Veracode State of Software Security reports, this feature supplement hones in particularly on the vulnerabilities in the software applications of publicly traded companies, following new SEC guidance issued in the US last year relating to disclosure of cybersecurity risks in company filings.

“Companies – particularly public ones – are beginning to be measured by regulators and investors on the strength of their cybersecurity solution and ability to protect intellectual property and customer data. This is a fundamental shift,” said Chris Wysopal, founder, CISO and CTO, Veracode.

“Companies can put all of the other cybersecurity controls in place but if there are application weaknesses, hackers have the will and time to find and exploit them. The issue simply can not be neglected anymore. Over the last year some of the most prominent breaches that were carried out against the most preeminent names in business took advantage of weaknesses in software applications to infiltrate traditional perimeter defence security controls. This should be a wake up call. Particularly in public company disclosures, the issue needs to be discussed in much more detail.”

Public companies fare no better than companies at large on software security or developer knowledge: Despite public companies having greater compliance requirements and usually more funding, only 16 percent of public company web applications passed initial testing compared to 14 percent for all companies at large – as measured by compliance against the OWASP Top 10 industry standard. The performance for non-web applications is worse for public companies, with 38 percent passing against the CWE/SANS industry standard opposed to 42 percent from all companies.

Reliance on third-party applications is widespread, but formal risk assessments are not: With many applications being bought as commercial-off-the-shelf applications, custom developed outsourced projects or software-as-a-service, managing the risks inherited from third parties is an important factor. However, only one in five public companies has performed a formal verification on a third-party application, suggesting they are operating under a false sense of security or making an assumption that

software procured from third-parties is secure upon entry.

Flat prevalence rates since 2012: With the two most frequently exploited vulnerability types - XSS and SQL injections - showing a statistically flat incidence rate from the first quarter of 2010 to the fourth quarter of 2011, the results suggest that new vulnerabilities are being introduced at the same rate as known vulnerabilities are being remediated.

Many companies defining custom policy chose to measure applications against PCI: Over 40 percent of public companies who defined a custom policy chose to measure their application against PCI or the OWASP Top 10 standard which underpins PCI. The main focus is on vulnerabilities that are most frequently exploited such as SQL Injection and Cross-site scripting.

Report Methodology

This Study of Software Related Cybersecurity Risks in Public Companies captures data collected from 126 public companies over the past 18 months from applications that were submitted to Veracode's cloud-based application security testing platform. These application s include both internally developed and those procured from third-party vendors.

One of the goals of the State of Software Security Report is to create greater awareness and security intelligence about the risks of unknown vulnerabilities lurking in everyday applications. The results are aimed at creating a greater sense of urgency around the problem of insecure software, while also giving organisations the information they need to quickly take action. Veracode also emphasises the ease with which organisations can incorporate software testing into current development cycles.

Download the Report

Veracode's Study of Software Related Cybersecurity Risks in Public Companies examines additional software security topics in context of application threat space trends, including details on the most commonly exploited vulnerabilities, risks associated with public company software applications, as well as factors driving application security policies in public companies. For complete report findings, download a copy of the report by visiting: http://www.veracode.com/soss

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 representing Global 2000 brands. For more information, visit www.veracode.com, follow on Twitter: @Veracode or read the Veracode Blog.

###

Media Contacts:
Ellen Moss (U.S.)
Weber Shandwick
617-520-7138
emoss@webershandwick.com

Fiona Bates (U.K.)
Weber Shandwick
0207 067 0703
fiona.bates@webershandwick.com