

Government and Private Enterprise Partner to Target Top Coding Flaws

Written By Jeffrey Bernstein

Published in February 2009 in MIS-ASIA

Many public-private partnership initiatives are contributing to the evolution of global information security risk mitigation. US-based InfraGuard and the Malaysia-based International Multilateral Partnership Against Cyber Threats (IMPACT) are two well-known examples.

In mid-January 2009, America's public-private partnership made a bold move by documenting and announcing the 25 most dominant coding flaws. The collaborative effort of government, academia and the commercial sector included participation from the National Security Agency and Department of Homeland Security in the US, along with a consortium of 30 other global information security organisations, including Symantec and Microsoft.

This move follows increasing levels of malicious cyber attacks targeted at the application layer and the valuable data that resides within it. Of equal concern is the increased pressure to protect the systems associated with command and control of electronic critical infrastructure. A review of 'reported' security breaches at the [Privacy Rights](#) website provides solid validation that year over year, malicious activity on the Internet continues to increase at an alarming rate. With this in mind, the coding flaw announcement is an industry-wide welcome breath of fresh air.

Issue categories

The newly announced list includes well-known flaws that can lead to, among others, successful Denial of Service (DoS) and Cross Site Scripting (XSS) exploits. The list is subdivided into the following three categories of issues:

1. Insecure Interaction Between Components - 9 errors
2. Risky Resource Management - 9 errors
3. Porous Defenses - 7 errors

The consortium's effort should be loudly applauded as widespread adoption and implementation appears imminent and will ultimately lead to lower rates of successful electronic compromise. It is widely expected that local, state, federal and international constituencies will establish contract clauses requiring all software vendors to be secured against the top 25 weakness list as an initial barrier to doing business. For example, New York State in the US has already drafted new procurement language mandating compliance from its vendors.

The idea of tracking most prevalent vulnerabilities has been around for years. Historically, security checklists have been a significant contributing factor to the heightening of security posture of network and application computing environments worldwide. In 2004, and perhaps the single defining precursor to the new top 25, the Open Source Web Application Security Project (OWASP) launched the 'OWASP Top 10' which was a similar effort to bring about awareness of key application coding flaws to a wide global audience. Driving attention

CRITICAL DEFENCE

through its worldwide reach of 130 member chapters, OWASP continues to make significant progress towards educating the private, commercial, education and government sectors. Early adopters of the OWASP criteria include the US Department of Defense, the US Federal Trade Commission (FTC), The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), British Telecom (BT) and the Payment Card Industry, as mandated by the PCI Standard, to name only a few.

Beginning in 2000, the SANS Institute and the National Infrastructure Protection Center (NIPC) began tracking the 'Top 10 Most Critical Security Vulnerabilities'. As the list gained in popularity, it came to be known as the 'SANS/FBI Top 20' and was segmented into three categories which covered 'General' Vulnerabilities, 'Windows' Vulnerabilities, and 'Unix' Vulnerabilities. CERT (Computer Emergency Response Team at Carnegie Mellon University with federal funding) also publishes a 'Top 10 Coding Flaw' reference list along with the various entries from the National Institute for Standards and Technology (NIST) which publishes more than 100 platform and system specific checklists that may be used in a similar fashion.

Increasing integration

Not surprisingly, open-source and third-party network and application scanning technology providers continue to integrate similar components within their wares. For instance, Qualys publishes a 'Top 10 Security Vulnerability' list which is updated monthly. The company and its competitors also offer modules that are designed specifically to address sector-specific vulnerabilities that are common to the banking, retail and utility space, among others. The latest version of Nessus includes a Supervisory Control and Data Acquisition (SCADA) 'plug-in' that can assess industrial control computer systems vulnerability from exploitation via the existence of known vulnerabilities.

The reason that security checklists are so popular is that the majority of successful system compromises can be traced to a limited number of exploits, vulnerabilities and flaws that the various 'top' and 'check' lists document. While small in number compared to the larger population count of actual issues, it is only a few software vulnerabilities which account for the majority of successful attacks. The reason is simply because the majority of attackers take the most convenient route to compromise. They exploit the best-known flaws using the most effective and widely available attack tools, betting that organisations that they target have not fixed the problems. In fact, SANS estimates that the issues, identified within the new top 25 coding list announced in January, are responsible for about 85 per cent of all malicious activity on the Internet.

This new coding flaw announcement is a major event for the development, security and end-user communities. Developers have a new functional guideline to better secure coding. The initiative is already heightening the awareness of the need to embed secure coding into the fabric of application development. Security assurance practitioners, auditors and assessors now have an added relevant reference point to assess and secure 'pre' and 'post' production code. End-users will benefit with the knowledge that the applications housing their sensitive data are stripped and hardened against what are considered the most common flaws, at any given time.

While the threat to data protection from application exploitation will remain among the most challenging security issues, the public-private application security partnership appears fired-up, vigilant and should be applauded for its early 2009 announcement.

*The 'Top 25 Most Dangerous Programming Errors' may be found at: <http://cwe.mitre.org/top25/#Brief>