

Issue 41

Publication date: 09/07/07

Contents

- Cyber Storm Warning
- SCADA & Control Systems Procurement Project
- The F-Secure Data Security Summary of January - June 2007
- Finding XSS & SQLI Vulnerabilities
- BITS Email Security Toolkit
- Getting Real about Security Governance
- New Version of Common Vulnerability Scoring System Released
- X-Morphic Exploitation
- The Vishing Guide

CCIP Contact Details:

T: +64 (0)4 498-7654
F: +64 (0)4 498-7655
E: info@ccip.govt.nz

<http://www.ccip.govt.nz/>

Cyber Storm Warning

M-Net

In March next year, New Zealand will be the target of an unprecedented cyber security attack on the country's critical infrastructure including utilities, central government and telecommunications networks. Experts say it will be unprecedented in terms of the severity, prolonged duration, co-ordination of minds behind it, and international collaboration surrounding the attack.

Source: <http://m-net.net.nz/1715/latest-news/latest-news/cyber-storm-warning.php>

SCADA & Control Systems Procurement Project

Multi-State Information Sharing and Analysis Center (MSISAC)

SCADA (Supervisory Control And Data Acquisition) generally refers to the systems which control our critical infrastructures -- such as electric power generators, traffic signals, dams, and other systems. Protecting our critical infrastructure and process control systems is a vital component of our nation's readiness and response efforts. The SCADA Procurement Project, established in March 2006, is a joint effort among public and private sectors focused on development of common procurement language that can be used by everyone. The goal is for federal, state and local asset owners and regulators to come together using these procurement requirements and to maximize the collective buying power to help ensure that security is integrated into SCADA systems.

Source: <http://www.msisac.org/scada/>

The F-Secure Data Security Summary of January - June 2007

F-Secure

Security threats cross technology borders towards a new malicious economy; social engineering, bank scams, Cyber War and clever mobile intruders

The F-Secure Lab saw a steady flow of reports on a vast variety of data security threats during the first half of 2007. The underlying trend to note is the spread of malicious activity across various forms of technology and applications during the 6-month period. It would appear that the parties behind orchestrating security attacks are conquering more and more foothold to build a stronger, sustainable commercial economy based on carefully crafted security attacks targeting consumers, companies and public sector organizations.

Source: http://www.f-secure.com/f-secure/pressroom/news/fs_news_20070613_1_eng.html

Finding XSS & SQLI Vulnerabilities

Secure Systems Lab, Vienna University of Technology

Cross-site scripting (XSS) and SQL injection (SQLI) vulnerabilities are present in many modern web applications, and are reported continuously on pages such as BugTraq. In the past, finding such vulnerabilities usually involved manual source code audits. Unfortunately, this manual vulnerability search is a very tiresome and error-prone task. Pixy is a Java program that performs automatic scans of PHP 4 source code, aimed at the detection of XSS and SQL injection vulnerabilities. Pixy takes a PHP program as input, and creates a report that lists possible vulnerable points in the program, together with additional information for understanding the vulnerability.

Source: <http://pixybox.seclab.tuwien.ac.at/pixy/index.php>

Information Security Links

Centre for the Protection of National Infrastructure (CPNI)

Canadian Cyber Incident Response Centre (CCIRC)

United States Computer Emergency Readiness Team (US-CERT)

CERT Coordination Center (CERT/CC)

Australian Computer Emergency Response Team (AusCERT)

Internet Storm Center (ISC)

US-CERT Cyber Security Bulletins

Safe Computing Links

The Internet Safety Group (NZ)

CCIP Security Tips

National Cyber Alert System (USA)

AusCERT National Information Technology Alert Service (AUS)

IT Security Awareness For Everyone (UK)

National Alerting Service (Netherlands)

BITS Email Security Toolkit

BITS

Email is now a primary means of communication from financial institutions to their customers and from financial institutions to other financial institutions and service providers. However, email is insecure and therefore fraught with risks. The medium lacks confidentiality and integrity unless uniform and explicit controls are put into place. Fraudsters and scammers are leveraging the convenience and cost-effectiveness of email to compromise the security of customer accounts and to undermine the reputations of financial institutions. While there are no “silver bullet” solutions, some of these risks can be mitigated by implementing existing technologies and protocols.

Source: <http://www.bitsinfo.org/downloads/Publications%20Page/BITSSecureEmailFINALAPRIL1507.pdf>

Getting Real about Security Governance

CERT/CC

For an organization that lacks a cohesive enterprise security governance program, establishing one may seem like an overwhelming endeavour. In fact, however, this is not the case. By breaking down enterprise security governance into its component activities, organizations can design and build a security governance program over time, tailoring it to suit their needs.

Source: <http://www.cert.org/podcast/show/losiallen.html>

New Version of Common Vulnerability Scoring System Released

Forum of Incident Response and Security Teams (FIRST)

Millions of computer users worldwide will enjoy more secure virtual experiences and transactions with the advent today of CVSSv2 – the latest version of the Common Vulnerability Scoring System. The release of version 2 was announced by the Forum of Incident Response and Security Teams (FIRST) and the Common Vulnerability Scoring System-Special Interest Group (CVSS-SIG). CVSS provides a universal open and standardized method for rating IT vulnerabilities.

Source: <http://www.first.org/cvss/>

X-Morphic Exploitation

IBM

Decades of malware development have been a source of innovation for today's Web browser exploit developers. Advanced malware techniques designed to bypass regular-expression and heuristic-based signature engines have been maturing for many years, and the lessons learned are now being applied to Web browser exploit development.

Source: http://www.iss.net/documents/whitepapers/IBM_ISS_x-morphic_exploitation.pdf

The Vishing Guide

IBM

Vishing is the practice of leveraging IP-based voice messaging technologies (primarily Voice over Internet Protocol, or VoIP) to socially engineer the intended victim into providing personal, financial or other confidential information for the purpose of financial reward. The term “vishing” is derived from a combination of “voice” and “phishing.”

Source: http://www.iss.net/documents/whitepapers/IBM_ISS_vishing_guide.pdf



While this e-bulletin is accurate to the best of our knowledge, CCIP does not accept any responsibility for errors or omissions. If any of the vulnerabilities affects you, you are advised to ensure that you have the most current information available. CCIP will not be liable for any loss or damage howsoever caused, arising from or in connection with the use of information contained in this e-bulletin.

CCIP only issues those external alerts that we assess as serious and would affect a large number of New Zealand users. For notification of all discovered software vulnerabilities we recommend that you subscribe to a commercial Computer Emergency Response Team or to vendor alert lists.

Reference in this e-bulletin in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions expressed herein may not be used for advertising or product endorsement purposes.