

Issue 83

Publication date: 13/08/2009

Contents

- Guidance Note on the Use of Portable Storage Devices
- Vulnerability Technical Reports
- Template Twitter Strategy for Government Departments
- Hacking Control System Web Applications with Nessus
- Cisco 2009 Midyear Security Report
- How Do We Deal with Fast Fluxing Cybercriminals?
- The Microsoft Office Visualization Tool (OffVis) Fact Sheet
- NIST Releases 'Historic' Final Version of Special Publication 800-53
- Release of SIFT Special Report: System Security Primer

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/>

Guidance Note on the Use of Portable Storage Devices

Privacy Commissioner

Portable Storage Devices (PSDs) are small, lightweight, portable, easy to use devices capable of storing and transferring large volumes of information. They include USB sticks, cell phones, iPods, PDAs (personal digital assistants), and smart phones such as BlackBerrys and iPhones. They are commonly used in both business and government, and widely used in the community. While advances in technology are transforming the way we work, it is easy to be blinded by the positives and fail to recognise and take account of the risks that the uses of PSDs also bring.

Source: <http://www.privacy.org.nz/>

Vulnerability Technical Reports

National Security Agency

These technical reports provide customers with valuable information regarding a variety of technologies. The reports may identify vulnerabilities and provide recommendations to improve or eliminate those vulnerabilities. The reports prioritize vulnerabilities in the reports and project future initiatives in that technology area.

Source: <http://www.nsa.gov/>

Template Twitter Strategy for Government Departments

Cabinet Office

You might think a 20-page strategy a bit over the top for a tool like Twitter. After all, microblogging is a low-barrier to entry, low-risk and low-resource channel relative to other corporate communications overheads like a blog or printed newsletter. And the pioneers in corporate use of Twitter by central government (see No 10, CLG and FCO) all started as low-profile experiments and grew organically into what they are today.

Source: <http://blogs.cabinetoffice.gov.uk/>

Hacking Control System Web Applications with Nessus

DigitalBond

We usually talk about Nessus in terms of vulnerability assessment or configuration auditing (i.e. identifying known vulnerabilities based on a set of signatures or identifying poor security configuration using audit files). Tenable recently expanded the Nessus web application testing plugins, however, that can help identify new or unknown vulnerabilities. The capability has been around for a while but recent updates have greatly enhanced it in terms of the types of tests and how you are able to control them. Couple that with another Tenable post about scanning embedded systems and you have some interesting control system implications.

Source: <http://www.digitalbond.com/>

Cisco 2009 Midyear Security Report

Cisco

The Cisco 2009 Midyear Security Report presents an overview of Cisco security intelligence, highlighting threat information and trends from the first half of 2009. The report also includes recommendations from Cisco security experts and predictions of how identified trends will evolve.

Source: <http://www.ciscozine.com/>

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

CCIP Security Guidelines

NetSafe

National Cyber Alert System (USA)

AusCERT National Information Technology Alert Service (AUS)

IT Security Awareness For Everyone (UK)

National Alerting Service (Netherlands)

How Do We Deal with Fast Fluxing Cybercriminals?

ICANN

Following a SSAC Advisory on Fast Flux Hosting and an Issues Report, the GNSO Council launched a Policy Development Process (PDP) on Fast Flux Hosting in May 2008. The Working Group published its Initial Report in January 2009, which discusses a series of questions about fast flux hosting and the range of possible answers developed by Working Group members. The Report also outlines potential next steps for Council deliberation. These next steps may include further work items for the Working Group or policy recommendations for constituency and community review and comment, and for Council deliberation.

Source: <http://www.icann.org/>

The Microsoft Office Visualization Tool (OffVis) Fact Sheet

Microsoft

The Microsoft Office Visualization Tool (OffVis) allows IT professionals, security researchers and malware protection vendors to better understand the Microsoft Office binary file format in order to deconstruct .doc-, .xls- and .ppt-based targeted attacks. The unique, easy-to-use tool offers a comprehensive view of any Microsoft Office binary file format sample simply by hovering a cursor over it. The tool then graphically shows important data structures and records for Microsoft Office Word, Microsoft Office PowerPoint and Microsoft Office Excel. Users can then browse and click through each record.

Source: <http://www.microsoft.com/>

NIST Releases 'Historic' Final Version of Special Publication 800-53

Government Computing News (US)

The National Institute of Standards and Technology has collaborated with the military and intelligence communities to produce the first set of security controls for all government information systems, including national security systems. The controls are included in the final version of Special Publication 800-53, Revision 3 "Recommended Security Controls for Federal Information Systems and Organizations," released Friday. NIST called the document historic.

Source: <http://gcn.com/>

Release of SIFT Special Report: System Security Primer

SIFT

SIFT has released its first Special Report of 2009. This paper was written to be a lightweight, easily adoptable system security primer and checklist to assist organisations in better understanding security requirements and controls. Using the techniques described in this primer will allow development teams to build a minimum level of security into a system without the overhead of incorporating an unwieldy process into the system development lifecycle or forcing large amounts of documentation upon system implementers.

Source: <http://www.sift.com.au/>



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.

