

## Issue 93

Publication date: 04/03/2010

### Contents

- DRAFT Guidelines for the Secure Deployment of IPv6
- Seeing NERC CIP through a Software Lens
- BackTrack 4 Final Release
- Top 25 Most Dangerous Programming Errors
- Welcome to the ZeuS Tracker
- The Tao of Signature Writing
- Traffic Talk: Testing Snort with Metasploit
- Report: Malicious PDF files comprised 80 percent of all exploits for 2009
- Good Practices Guide for Deploying DNSSEC

### CCIP Contact Details:

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

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

## DRAFT Guidelines for the Secure Deployment of IPv6

*NIST*

NIST announces the public comment release of Special Publication (SP) 800-119, Guidelines for the Secure Deployment of IPv6. IPv6 (Internet Protocol version 6) is the next generation Internet Protocol, accommodating vastly increased address space. This document describes and analyzes IPv6's new and expanded protocols, services, and capabilities, including addressing, DNS, routing, mobility, quality of service, multihoming, and IPsec. For each component, there is a detailed analysis of the differences between IPv4 and IPv6, the security ramifications and any unknown aspects. It characterizes new security threats posed by the transition to IPv6 and provides guidelines on IPv6 deployment, including transition, integration, configuration, and testing. It also addresses more recent significant changes in the approach to IPv6 transition.

Source: <http://csrc.nist.gov/>

## Seeing NERC CIP through a Software Lens

*Smart Grid Security Blog*

Thinking about the future grid, AMI and Smart Grid systems can get so complicated that they can be difficult to conceptualize unless you use a construct that limits the scope of what's being considered. Given that so much of the Smart Grid "smarts" involves new applications and other advances in software, an important way to think about NERC CIP and your organization is to focus on your software assets.

Source: <http://smartgridsecurity.blogspot.com/>

## BackTrack 4 Final Release

*backtrack-linux.org*

BackTrack is a Linux-based penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. Regardless if you're making BackTrack your primary operating system, booting from a LiveDVD, or using your favorite thumbdrive, BackTrack has been customized down to every package, kernel configuration, script and patch solely for the purpose of the penetration tester.

Source: <http://www.backtrack-linux.org/>

## Top 25 Most Dangerous Programming Errors

*CWE/SANS*

The 2010 CWE/SANS Top 25 Most Dangerous Programming Errors is a list of the most widespread and critical programming errors that can lead to serious software vulnerabilities. They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.

Source: <http://cwe.mitre.org/>

### 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)

## Welcome to the ZeuS Tracker

*abuse.ch*

The ZeuS Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have any questions please take a look into the FAQ or send me a email (contact).

Source: <https://zeustracker.abuse.ch/>

## The Tao of Signature Writing

*Signature Analyst*

Signature generation, analysis and testing is a complex art, that requires many parameters to be coordinated. "Tao" is "the ultimate principle of the universe", and in here it means that signature writing requires an analyst to understand the principles in the signature universe. Since each signature format has its own structural design and components to perform pattern matching of the exploit or malicious software/code from entering into the network, one has to know the entire signature universe on the whole and how it interacts with the other universe.

Source: <http://sign.kaffenews.com/>

## Traffic Talk: Testing Snort with Metasploit

*SearchNetworkingChannel.com*

In this tip from Richard Bejtlich, solution providers whose customers are wondering whether their solutions are working as expected can learn how to deliver on what was promised by testing Snort, the network intrusion detection system (IDS). Testing Snort with Metasploit can help avoid poor testing and ensure that your customers' networks are protected.

Source: <http://searchnetworkingchannel.techtarget.com/>

## Report: Malicious PDF files comprised 80 percent of all exploits for 2009

*Dancho Danchev*

A newly released report shows that based on more than a trillion Web requests processed in 2009, the use of malicious PDF files exploiting flaws in Adobe Reader/Adobe Acrobat not only outpaced the use of Flash exploits, but also, grew to 80% of all exploits the company encountered throughout the year.

Source: <http://blogs.zdnet.com/>

## Good Practices Guide for Deploying DNSSEC

*ENISA*

Deploying DNSSEC requires a number of security details and procedures to be defined and followed with specific requirements as to timing. This guide addresses these issues from the point of view of information security managers responsible for defining a policy and procedures to secure the DNS services of a company or an organisation, and from the point of view of competent authorities defining or regulating requirements for deployment.

Source: <http://www.enisa.europa.eu/>



*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.*

