

HNS Newsletter
Issue 277 - 08.08.2005.
<http://net-security.org>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week.

InfoSec Research Library - <http://net-security.bitpipe.com>

In association with BitPipe, Help Net Security is giving you a possibility to freely read the latest white papers, case studies, webcasts and product information related to information security.

Some of the topics covered include: Authentication, Email Security, Identity Management, Network Security, Security Policies. VPN and Wireless Security.

Point your browsers to: <http://net-security.bitpipe.com>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Software
- 6) Conferences
- 7) Security World
- 8) Virus News

[Security news]

A HACKER GAMES THE HOTEL

A vulnerability in many hotel television infrared systems can allow a hacker to obtain guests' names and their room numbers from the billing system.

<http://www.net-security.org/news.php?id=8432>

CISCO, SECURITY RESEARCHER SETTLE DISPUTE

Cisco Systems Inc. and a network security firm reached a settlement Thursday with a researcher who quit his job so he could deliver a speech on a serious flaw in Cisco software that routes data over the Internet.

<http://www.net-security.org/news.php?id=8433>

WORM MOCKS CONVICTED SASSER AUTHOR

A new virus mocking the creator of the Sasser worm is spreading

across the net.

<http://www.net-security.org/news.php?id=8434>

IDC SLAMS EUROPEAN FIRMS' ATTITUDES TO SECURITY

IDC says that to date, most organisations have had a lacklustre approach to IT security in Western Europe.

<http://www.net-security.org/news.php?id=8435>

GETTING A SECURE HANDLE ON HANDHELDS

Cell phones, smart phones, and PDAs find their way into the workforce when employees buy them and use them without regard to official company and security policies.

<http://www.net-security.org/news.php?id=8436>

WINDOWS COPY PROTECTION DEFEATED

Single line of JavaScript all that is needed.

<http://www.net-security.org/news.php?id=8437>

IS VOIP SECURE ENOUGH FOR PRIME TIME?

VoIP is hot, but VoIP security is not.

<http://www.net-security.org/news.php?id=8438>

ISS PURSUES LYNN PRESENTATION COPIES

ISS is now pursuing Web sites posting Mike Lynn's presentation.

<http://www.net-security.org/news.php?id=8439>

THE SORRY STATE OF IM SECURITY

With more than 2,000 percent year-on-year growth rate in IM threats, somebody's got to see a huge opportunity.

<http://www.net-security.org/news.php?id=8440>

DARK TRAFFIC EMAIL REPORT

This report defines and analyzes dark traffic email gathered through a combination of research interviews with enterprise IT and email administrators in the US.

<http://www.net-security.org/news.php?id=8441>

EARS RECOMMENDED FOR BIOMETRICS

A scientist in the UK has proposed that the unique pattern inside each individual's ear could be used as a biometric identifier, in the same way fingerprints are used.

<http://www.net-security.org/news.php?id=8442>

BUMBLEBEE WI-FI SPECTRUM ANALYZER

Berkeley analyzer precisely discovers wireless and RF interference but lacks full-spectrum support.

<http://www.net-security.org/news.php?id=8443>

FEDS EYE NEW MISSION: ZOMBIE HUNTING

According to Prolexic Technologies, an intrusion prevention and detection firm based in Hollywood, Fla., America Online is the most targeted ISP in the U.S., with 11.7 percent of all zombie attacks being pointed at AOL. This was followed by Comcast.net, which is the target of 10.66 percent of would-be zombie planters.
<http://www.net-security.org/news.php?id=8444>

RESEARCHER DESCRIBES HOW THE PHISHING ECONOMY WORKS

Phishers use Internet chat to communicate with each other and buy and sell victims' financial information.
<http://www.net-security.org/news.php?id=8445>

CYBER BLACKMAILERS AND ADWARE THREATEN

Increases in the number of cyber blackmailers and adware going 'deep' are just some of the highlights in the April-June 2005 Malware report from Alexander Gostev, senior virus analyst, Kaspersky Lab.
<http://www.net-security.org/news.php?id=8446>

BLACKHAT: FIRST JERICHO FORUM CHALLENGE WINNERS ANNOUNCED

Researchers from a Swedish security software house have scooped the first Jericho Forum Challenge at the BlackHat convention in Las Vegas.
<http://www.net-security.org/news.php?id=8447>

LINUX SECURITY - IS IT READY FOR THE AVERAGE USER?

There seems to be a new important security patch out for Linux every month, lots of "do not use this program" warnings, too many articles and books with too little useful information, high-priced consultants, and plenty of talk about compromised systems. It is almost enough to send someone back to Windows. Can the average Linux user or system administrator keep his or her system secure and still have time to do other things? Bob Toxen is happy to say yes and here is how to do it.
<http://www.net-security.org/news.php?id=8448>

MICROSOFT ANTI-PHISHING WHITE PAPER

The focus of this white paper is to describe the basic workings of a new capability, the Microsoft Phishing Filter, that will be included in the upcoming release of Internet Explorer 7.
<http://www.net-security.org/news.php?id=8449>

ASSESS SYSTEM SECURITY USING A LINUX LIVECD

Four LiveCD offerings specialize in nailing down vulnerabilities.
<http://www.net-security.org/news.php?id=8450>

THE CARDSYSTEMS BLAME GAME

Hiring a security auditor in light of the CardSystems breach reveals quite a bit about the legal side of security consultants.
<http://www.net-security.org/news.php?id=8451>

WHAT TO DO BEFORE AN IOS DISASTER STRIKES
Security expert Jian Zhen explains how to fend off a Cisco router exploit.
<http://www.net-security.org/news.php?id=8452>

OPEN SPECIFICATION TO AID PC SERVER SECURITY
The Trusted Computing Group has announced an open specification for trusted servers to allow manufacturers to improve hardware security on PC servers.
<http://www.net-security.org/news.php?id=8453>

TWO EXPERTS DISCUSS BIOMEDICINE, CYBERWARFARE, AND SECURITY
There have always been similarities and overlap between the worlds of biology and computer science. Nowhere is this more evident than in computer security, where the basic terminology of viruses and infection is borrowed from biomedicine.
<http://www.net-security.org/news.php?id=8454>

HOW TO PROTECT DATA RESIDING ON YOUR IP NETWORK
Attend this webcast for discussion of the topics, overview of typical IP Network attacks, why a layered defense is critical and the importance of data encryption.
<http://www.net-security.org/news.php?id=8455>

MICROSOFT AIMS TO HOST REGULAR HACKER MEETINGS
Microsoft is working on plans to make a recent hacker meeting held on its Washington, campus a twice-yearly event, according to a spokesman for the vendor's security group.
<http://www.net-security.org/news.php?id=8456>

REVIEW: ZONEALARM INTERNET SECURITY SUITE 6.0
We've long been users of Zone Labs' ZoneAlarm products due to their ease of use, effectiveness and excellent value for money. ZoneAlarm Internet Security Suite 6.0 is no different.
<http://www.net-security.org/news.php?id=8457>

SOFTWARE PIRATES TAP INTO TECHNOLOGY
Criminal gangs are increasing taking advantage of the internet to peddle counterfeit software, say experts.
<http://www.net-security.org/news.php?id=8458>

HACKERS DEMONSTRATE THEIR SKILLS IN VEGAS
Even allegedly foolproof biometrics aren't totally safe at Defcon, the conference where crackers, hackers, and feds come to share tips

and tricks.

<http://www.net-security.org/news.php?id=8459>

HOW TO DEVELOP A SECURITY TRAINING PROGRAM THAT WORKS

The program can be customized for your organization by hiring specialized training consultants or by using internal staff knowledgeable in system and user vulnerabilities and exploitable areas.

<http://www.net-security.org/news.php?id=8460>

INSTALLING AND CONFIGURING MICROSOFT'S DATA PROTECTION MANAGER, PART 2

In this two part article, we show you how to install and configure DPM and evaluate how this can be integrated into your overall security strategy.

<http://www.net-security.org/news.php?id=8461>

THE SHMOO BLOODHOUND WI-FI GUN

This is a low cost "gun" made from a Pocket PC and some off the shelf parts that can find rouge Wireless access points.

<http://www.net-security.org/news.php?id=8462>

INTERFERENCE, NOT HACKING, SAID TO BE BIGGEST WIRELESS THREAT AT DEFCON

The biggest wireless threat at the recent DefCon conference came from items like microwave ovens according to AirMagnet.

<http://www.net-security.org/news.php?id=8463>

AUTOMATED BACKUPS ON TIGER USING RSYNC

In this article I'm going to show you how to create a free, customizable backup solution using only software that comes with Mac OS X 10.4, which will automatically back up changes to your data without user intervention.

<http://www.net-security.org/news.php?id=8464>

AUTHENTICATION AUDITING IN WINDOWS 2000

Authentication auditing is an essential part of protecting your Windows computers from intrusion.

<http://www.net-security.org/news.php?id=8465>

APPLE ADOPTS CONTROVERSIAL SECURITY CHIP

PM to limit OS X to Macs, but could to more.

<http://www.net-security.org/news.php?id=8466>

IBM: SECURITY ATTACKS UP 50%

Criminal-driven security attacks and emails with viruses increased by 50% in the first half of this year according to a report released by IBM.

<http://www.net-security.org/news.php?id=8467>

ANALYSTS SAY ATM SYSTEMS HIGHLY VULNERABLE

By failing to scan security codes in the magnetic strips on ATM and debit cards, many banks are letting thieves get away with an increasingly common fraud at a cost of several billion dollars a year.

<http://www.net-security.org/news.php?id=8468>

MORE RESOURCES ON CISCOGATE

The media is now calling the Lynn affair "Ciscogate."

<http://www.net-security.org/news.php?id=8469>

BLUETOOTH SECURITY - THE CAR WHISPERER

The Car Whisperer and allows people equipped with a Linux Laptop and a directional antenna to inject audio to, and record audio from bypassing cars that have an unconnected Bluetooth handsfree unit running.

<http://www.net-security.org/news.php?id=8470>

HACKERS CASH IN ON 802.1X CONFUSION

New standard has a way to go.

<http://www.net-security.org/news.php?id=8471>

US RAISE FRESH CYBER-TERROR CLAIMS

Cyber terrorists are attempting to penetrate government networks using the same methods as internet hackers and many nations are vulnerable to the threat, a US State Department official said.

<http://www.net-security.org/news.php?id=8472>

HACKED: WHO ELSE IS USING YOUR COMPUTER?

This article brings to light how people tend to be complacent with their computers and not understand the little things they have overlooked that have left themselves open to others on the Internet.

<http://www.net-security.org/news.php?id=8473>

BUG FIXES, SECURITY SUPPORT TO BE TOP PRIORITY IN IE 7

Microsoft plans to add support for cascading style sheets in the upcoming Internet Explorer 7, but other standards will take a back seat to critical bug fixes.

<http://www.net-security.org/news.php?id=8474>

FILE-COMPRESSION TOOL HIDES UGLY SECURITY FLAW

A buffer overflow vulnerability in Zlib could give attackers an opening on unpatched Linux and BSD systems.

<http://www.net-security.org/news.php?id=8475>

CISCO WEBSITE BREACHED, PASSWORDS RESET

Security at Cisco Systems remained front and centre as the company confirmed that it had to reset all passwords to its website because of a vulnerability in the search tool at Cisco.com.

<http://www.net-security.org/news.php?id=8476>

LINUX KERNEL QUALITY, SECURITY SHOWS IMPROVEMENT

A new study released today by code-analysis tools maker Coverity Inc. finds that overall quality and security of the Linux kernel has improved substantially in the last six months.

<http://www.net-security.org/news.php?id=8477>

KEY MANAGEMENT HOLDING BACK ENCRYPTION

Businesses are keener than ever to roll out data encryption, but are still struggling with the complexity of key management, a new survey has concluded.

<http://www.net-security.org/news.php?id=8478>

AN IT MANAGER'S GUIDE TO PROVISIONING AND IDENTITY MANAGEMENT

With staff now requiring access to so many internal and external computer systems, all of which might require separate usernames, passwords and access privileges, identity management is far from straightforward. Learn what can be done to simplify identity management in this article.

<http://www.net-security.org/news.php?id=8479>

LOGGING AND MONITORING APACHE (PART 1)

Most administrators do not think about the logs much before an intrusion happens and only realize their configuration mistakes when it is discovered that critical forensic information is not available.

<http://www.net-security.org/news.php?id=8480>

SPEAR PHISHERS LAUNCH TARGETED ATTACKS

Customised malware attacks are becoming more commonplace with virus-laden emails up 50 per cent in the first half of 2005 despite a decrease in volumes of spam and simple computer viruses, according to an IBM security report.

<http://www.net-security.org/news.php?id=8481>

MIKE LYNN'S 'EXPLOIT', IN PLAIN (NON-TECHNICAL) ENGLISH

here has been an almost unbelievable amount of hubbub lately about the research that Mike Lynn gave a demonstration of at the BlackHat conference last week, and there's been a positively dizzying amount of "spin" applied to the media.

<http://www.net-security.org/news.php?id=8482>

SETTING UP SSL CONNECTIONS

The ability to remotely access business information can present opportunities for unauthorized access to information, data theft, or

cyber attacks.

<http://www.net-security.org/news.php?id=8483>

ROOTING THE FORTUNE 100

Blackhat is one of my favorite places to do some casual online banking over an insecure WiFi connection. Where's the risk, right? All joking aside, Blackhat is in fact a great place to do some deep thought on the current state of the security industry.

<http://www.net-security.org/news.php?id=8484>

EXPLORING SPYWARE AND ADWARE RISK ASSESSMENT

This paper posits a working definition of spyware and adware, and outlines suggestions for evaluating tests of spyware and adware protection.

<http://www.net-security.org/news.php?id=8485>

PHISHERS HACK EBAY

Link takes victims to real eBay sign-in page, then hidden characters redirect to scam site.

<http://www.net-security.org/news.php?id=8486>

HOW ENDPOINT SECURITY WORKS

If you are interested in using VPNs nowadays, you should also be interested in using endpoint security.

<http://www.net-security.org/news.php?id=8487>

PALLADIUM NOT IN APPLE DEV KITS AFTER ALL

Earlier reports circulating around the Internet concerning Apple's inclusion of a Trusted Platform Module (TPM) chip in Intel-based Macs were incorrect.

<http://www.net-security.org/news.php?id=8488>

VOIP SECURITY THREATS: FACT OR FICTION?

Currently VoIP security isn't a concern for most I.T. managers, but that will quickly change once companies start publicizing their SIP addresses in VoIP communications, on business cards and Web sites.

<http://www.net-security.org/news.php?id=8489>

AUDITING USER ACCOUNTS

This article will discuss the key user account properties that need to be audited, as well as the tools that can help complete the task.

<http://www.net-security.org/news.php?id=8490>

HACKER FEAR FUELS OUTSOURCED SECURITY SPEND

Complexity of deploying in-house security systems also boosting services.

<http://www.net-security.org/news.php?id=8491>

PIRACY COUPLE GETS JAIL SENTENCE

A married couple arrested for music, film and game piracy have received jail terms of between six and 21 months.

<http://www.net-security.org/news.php?id=8492>

SSL ENCRYPTED SYSLOG WITH STUNNEL

In this paper, I describe how to write syslog messages to a MySQL database.

<http://www.net-security.org/news.php?id=8493>

ONE IN FIVE HIT BY IDENTITY THEFT

Experian-Gallup report warns of growing danger.

<http://www.net-security.org/news.php?id=8494>

RACKSPACE ILLEGALLY HANDED CUSTOMER DATA TO FBI

Hosting provider Rackspace acted illegally in handing over the London-based servers hosting the websites for Indymedia.org to US authorities.

<http://www.net-security.org/news.php?id=8495>

ADAPTING TO THE CHANGING LANDSCAPE OF SECURITY

Read this white paper to learn about the changing landscape of security and explore ways to re-examine your business' processes. In addition, this paper provides guidelines for evaluating competing security solutions.

<http://www.net-security.org/news.php?id=8496>

10 TIPS FOR PREPARING AND PASSING THE CISSP EXAM

Insights, tips and tricks from a CISSP for putting your best foot forward when you sit this grueling, six-hour security theory exam.

<http://www.net-security.org/news.php?id=8497>

WINDOWS SYSCALL SHELLCODE

This article has been written to show that is possible to write shellcode for Windows operating systems that doesn't use standard API calls at all.

<http://www.net-security.org/news.php?id=8498>

COURT ORDERS CARDSYSTEMS TO RETAIN BREACH INFORMATION

Evidence needed in case of 40M exposed credit card numbers.

<http://www.net-security.org/news.php?id=8499>

CAN-SPAM OR CANNOT, THAT IS THE QUESTION

The court determined that White Buffalo complied with federal law, that its e-mails were not illegal, but the law applies to the University of Texas as it would to an Internet service provider that employs protection measures.

<http://www.net-security.org/news.php?id=8500>

SIX MICROSOFT PATCHES ON THE WAY

Microsoft is set to release six patches on Tuesday for its Windows operating system.

<http://www.net-security.org/news.php?id=8501>

SILENT, DEADLY FORMS OF PHISHING DOUBLE

While the number of phishing scam Web sites stayed relatively flat in June, the most malicious form of Internet ID thievery has doubled in just three months.

<http://www.net-security.org/news.php?id=8502>

WINDOWS VISTA ALREADY UNDER VIRUS ATTACK

Proof-of-concept code exploits upcoming MSH scripting technology.

<http://www.net-security.org/news.php?id=8503>

RSS BEHIND THE FIREWALL

NewsGator Technologies introduced Enterprise Server on Thursday, a business-class application for enabling RSS content delivery behind the firewall.

<http://www.net-security.org/news.php?id=8504>

ROOTKIT BATTLE: ROOTKIT REVEALER VS. HACKER DEFENDER

Although rootkits have been threatening various platforms for years, only recently did a major battle develop between the rootkit creators and eradicators.

<http://www.net-security.org/news.php?id=8505>

[Vulnerabilities]

All vulnerabilities are located here:

<http://www.net-security.org/vulnerabilities.php>

web content management AddModifyInput.php Remote Privilege Escalation

<http://www.net-security.org/vulnerability.php?id=18524>

Linux dump flock() /etc/dumpdates Local DoS

<http://www.net-security.org/vulnerability.php?id=18531>

Karrigell Python Namespace Arbitrary Command Execution
<http://www.net-security.org/vulnerability.php?id=18506>

Naxtor e-directory admin/default.asp Password Field SQL Injection
<http://www.net-security.org/vulnerability.php?id=18502>

Naxtor e-directory signin.asp Password Field SQL Injection
<http://www.net-security.org/vulnerability.php?id=18503>

Naxtor e-directory message.asp message Variable XSS
<http://www.net-security.org/vulnerability.php?id=18504>

UnZip Race Condition Arbitrary File Permission Modification
<http://www.net-security.org/vulnerability.php?id=18530>

Phorum file.php SQL Injection
<http://www.net-security.org/vulnerability.php?id=18496>

Phorum search.php XSS
<http://www.net-security.org/vulnerability.php?id=18497>

Debian apt-cacher Unspecified Arbitrary Remote Command Execution
<http://www.net-security.org/vulnerability.php?id=18500>

Metasploit Framework msfweb Defanged Mode Remote Bypass
<http://www.net-security.org/vulnerability.php?id=18495>

OpenBook admin.php Multiple Field SQL Injection
<http://www.net-security.org/vulnerability.php?id=18475>

ChurchInfo Canvas05Editor.php FamilyID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18408>

ChurchInfo CanvasEditor.php FamilyID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18409>

ChurchInfo ClassAttendance.php GroupID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18410>

ChurchInfo DepositSlipEditor.php DepositSlipID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18411>

ChurchInfo FamilyView.php FamilyID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18412>

ChurchInfo GroupDelete.php GroupID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18413>

ChurchInfo GroupMemberList.php GroupID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18414>

ChurchInfo GroupPropsEditor.php PersonID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18415>

ChurchInfo GroupReport.php GroupID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18416>

ChurchInfo GroupView.php GroupID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18417>

ChurchInfo MemberRoleChange.php Multiple Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18418>

ChurchInfo PDFLabel.php PersonID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18419>

ChurchInfo PersonView.php PersonID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18420>

ChurchInfo PledgeDetails.php PledgeID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18421>

ChurchInfo PropertyAssign.php PersonID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18422>

ChurchInfo PropertyEditor.php PropertyID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18423>

ChurchInfo QueryView.php Multiple Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18424>

ChurchInfo SelectDelete.php Number Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18425>

ChurchInfo SelectList.php Number Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18426>

ChurchInfo UserDelete.php PersonID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18427>

ChurchInfo WhyCameEditor.php PersonID Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18428>

ChurchInfo Canvas05Editor.php FamilyID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18429>

ChurchInfo CanvasEditor.php FamilyID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18430>

ChurchInfo ClassAttendance.php GroupID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18431>

ChurchInfo ClassList.php GroupID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18432>

ChurchInfo ConfirmLabels.php GroupID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18433>

ChurchInfo DirectoryReport.php GroupID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18434>

ChurchInfo FamilyView.php FamilyID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18435>

ChurchInfo GroupPropsFormRowOps.php GroupID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18436>

ChurchInfo NewsLetterLabels.php GroupID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18437>

ChurchInfo PledgeDetails.php PledgeID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18438>

ChurchInfo PropertyEditor.php PropertyID Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18439>

ChurchInfo UserDelete.php Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18450>

PHPFreeNews Footer.php ScriptVersion Variable XSS
<http://www.net-security.org/vulnerability.php?id=18451>

PHPFreeNews ScriptFunctions.php Multiple Variable XSS
<http://www.net-security.org/vulnerability.php?id=18452>

PHPFreeNews Logout.php Arbitrary Site Redirect
<http://www.net-security.org/vulnerability.php?id=18453>

PHPFreeNews /inc/ Multiple Script Direct Request Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18454>

PHPFreeNews admin.php Information Disclosure
<http://www.net-security.org/vulnerability.php?id=18455>

PHPFreeNews Default Admin Account Password
<http://www.net-security.org/vulnerability.php?id=18456>

PHPFreeNews Login password Field SQL Injection
<http://www.net-security.org/vulnerability.php?id=18457>

FlexPHPNews index.php Multiple Variable XSS
<http://www.net-security.org/vulnerability.php?id=18486>

FlexPHPNews news.php Multiple Variable XSS
<http://www.net-security.org/vulnerability.php?id=18487>

FlexPHPNews search.php Multiple Variable XSS
<http://www.net-security.org/vulnerability.php?id=18488>

FlexPHPNews catalog.php Multiple Variable XSS
<http://www.net-security.org/vulnerability.php?id=18489>

FlexPHPNews usercheck.php logincheck Variable Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18490>

FlexPHPNews news.php Large Value DoS
<http://www.net-security.org/vulnerability.php?id=18491>

FlexPHPNews usercheck.php Admin Login Multiple Field SQL Injection
<http://www.net-security.org/vulnerability.php?id=18492>

Multiple Gopher Client Insecure Temporary File Creation Privilege Escalation
<http://www.net-security.org/vulnerability.php?id=18390>

Ragnarok Online Control Panel Apache Authentication Bypass
<http://www.net-security.org/vulnerability.php?id=18389>

BusinessMail SMTP Multiple Command Remote Overflow DoS
<http://www.net-security.org/vulnerability.php?id=18407>

Kayako LiveResponse index.php username Variable XSS
<http://www.net-security.org/vulnerability.php?id=18395>

Kayako LiveResponse index.php Calendar Feature Multiple Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=18396>

Kayako LiveResponse Unspecified Script Injection Privilege Escalation
<http://www.net-security.org/vulnerability.php?id=18397>

Kayako LiveResponse index.php Plaintext Password Disclosure
<http://www.net-security.org/vulnerability.php?id=18398>

Kayako LiveResponse Include Scripts Direct Request Path Disclosure
<http://www.net-security.org/vulnerability.php?id=18399>

MySQL Eventum view.php id Variable XSS
<http://www.net-security.org/vulnerability.php?id=18400>

MySQL Eventum list.php release Variable XSS
<http://www.net-security.org/vulnerability.php?id=18401>

MySQL Eventum get_jsrs_data.php F Variable XSS
<http://www.net-security.org/vulnerability.php?id=18402>

MySQL Eventum login.php email Variable SQL Injection Authentication Bypass
<http://www.net-security.org/vulnerability.php?id=18403>

MySQL Eventum custom_fields.php SQL Injection

<http://www.net-security.org/vulnerability.php?id=18404>

MySQL Eventum custom_fields_graph.php SQL Injection
<http://www.net-security.org/vulnerability.php?id=18405>

MySQL Eventum releases.php SQL Injection
<http://www.net-security.org/vulnerability.php?id=18406>

[Advisories]

All advisories are located at:
http://www.net-security.org/archive_advi.php

Trustix Secure Linux Security Advisory - bzip2, perl-compress-zlib,
proftpd (2005-0040)
<http://www.net-security.org/advisory.php?id=5123>

Mandriva Linux Security Update Advisory - ethereal (MDKSA-2005:131)
<http://www.net-security.org/advisory.php?id=5122>

Ubuntu Security Notice - bzip2 vulnerability (USN-161-1)
<http://www.net-security.org/advisory.php?id=5121>

Conectiva Linux Security Announcement - kopete (CLA-2005:989)
<http://www.net-security.org/advisory.php?id=5120>

Conectiva Linux Security Announcement - kde (CLA-2005:990)
<http://www.net-security.org/advisory.php?id=5119>

Conectiva Linux Security Announcement - heartbeat (CLA-2005:991)
<http://www.net-security.org/advisory.php?id=5118>

Conectiva Linux Security Announcement - kde (CLA-2005:988)
<http://www.net-security.org/advisory.php?id=5117>

SUSE Security Announcement - kernel (SUSE-SA:2005:044)
<http://www.net-security.org/advisory.php?id=5116>

Mandriva Linux Security Update Advisory - apache (MDKSA-2005:130)
<http://www.net-security.org/advisory.php?id=5115>

Mandriva Linux Security Update Advisory - apache2 (MDKSA-2005:129)
<http://www.net-security.org/advisory.php?id=5114>

Mandriva Linux Security Update Advisory - mozilla (MDKSA-2005:128)
<http://www.net-security.org/advisory.php?id=5113>

Debian Security Advisory - apt-cacher (DSA 772-1)
<http://www.net-security.org/advisory.php?id=5112>

Trustix Secure Linux Security Advisory - mysql, fetchmail, zlib,
perl, apache, netpbm, vim, nss_ldap (2005-0038)
<http://www.net-security.org/advisory.php?id=5111>

Ubuntu Security Notice - unzip vulnerability (USN-159-1)
<http://www.net-security.org/advisory.php?id=5110>

Ubuntu Security Notice - gzip vulnerability (USN-158-1)
<http://www.net-security.org/advisory.php?id=5109>

Debian Security Advisory - pdns (DSA 771-1)
<http://www.net-security.org/advisory.php?id=5108>

Ubuntu Security Notice - mozilla-thunderbird vulnerabilities
(USN-157-1)
<http://www.net-security.org/advisory.php?id=5107>

[Articles]

All articles are located at:
http://www.net-security.org/articles_main.php

Articles can be contributed to articles@net-security.org

AN IT MANAGER'S GUIDE TO PROVISIONING AND IDENTITY MANAGEMENT
With staff now requiring access to so many internal and external

computer systems, all of which might require separate usernames, passwords and access privileges, identity management is far from straightforward. Learn what can be done to simplify identity management in this article.

<http://www.net-security.org/article.php?id=810>

LINUX SECURITY - IS IT READY FOR THE AVERAGE USER?

There seems to be a new important security patch out for Linux every month, lots of "do not use this program" warnings, too many articles and books with too little useful information, high-priced consultants, and plenty of talk about compromised systems. It is almost enough to send someone back to Windows. Can the average Linux user or system administrator keep his or her system secure and still have time to do other things? I am happy to say yes and here is how to do it.

<http://www.net-security.org/article.php?id=809>

[Software]

Windows software is located at:

http://net-security.org/software_main.php?cat=1

Linux software is located at:

http://net-security.org/software_main.php?cat=2

Pocket PC software is located at:

http://net-security.org/software_main.php?cat=3

Mac OS X software is located at:

http://net-security.org/software_main.php?cat=5

ACUNETIX WEB VULNERABILITY SCANNER 2.0 (Windows)

This tool can automatically audit the security of your website and web applications.

<http://www.net-security.org/software.php?id=633>

AIRSCANNER MOBILE FIREWALL 2.4 (Pocket PC)

Airscanner Mobile Firewall is a full-strength, fully configurable, NDIS packet-filtering TCP/IP firewall.

<http://www.net-security.org/software.php?id=573>

BASTILLE LINUX 3.0.7 (Linux)

The Bastille Hardening System attempts to "harden" or "tighten" the Linux operating system.

<http://www.net-security.org/software.php?id=217>

CONFIDENTIAL NOTES 1.1 (Pocket PC)

Confidential Notes is a practical and easy to use solution that increases your productivity and provides you with a high level of security for your mobile data.

<http://www.net-security.org/software.php?id=632>

ISTUMBLER 95 (Mac OS X)

iStumbler is a free, open source tool for finding AirPort networks, Bluetooth devices and now mDNS services with your Mac.

<http://www.net-security.org/software.php?id=620>

MAILSCANNER 4.44.6 (Linux)

MailScanner is a virus scanner for e-mail designed for use on e-mail gateways.

<http://www.net-security.org/software.php?id=144>

NAGIOS 2.0b4 (Linux)

Nagios is a host and service monitor designed to inform you of network problems before your clients, end-users or managers do.

<http://www.net-security.org/software.php?id=279>

PRELUDE MANAGER 0.9.0 RC7 (Linux)

Prelude Manager is the main program of the Prelude Hybrid IDS suite.

<http://www.net-security.org/software.php?id=264>

PROSHIELD 3.7.23 (Linux)

ProShield is a security program for Debian Linux.

<http://www.net-security.org/software.php?id=282>

REVELATION 0.4.4 (Linux)

Revelation is a password manager for the GNOME 2 desktop.

<http://www.net-security.org/software.php?id=293>

TOR 0.1.0.14 alpha (Windows)

An anonymous Internet communication system.

<http://www.net-security.org/software.php?id=253>

VISUALROUTE 2005 9.3f (Windows)

VisualRoute delivers the functionality of key Internet "ping," "whois," and "traceroute" tools, in a high-speed visually integrated package.

<http://www.net-security.org/software.php?id=2>

WIFI GRAPH 0.3 RC3 (Pocket PC)

WiFi Graph let you spot neighboring Wireless LAN Access Points and their connectivity.
<http://www.net-security.org/software.php?id=634>

[Conferences]

All conferences are located at:
<http://net-security.org/conferences.php>

Crypto 2005
Organized by International Association for Cryptologic Research - 14 August-18 August 2005
<http://www.net-security.org/conference.php?id=122>

8th Information Security Conference(ISC'05)
Organized by Institute for Infocomm Research - 21 September-23 September 2005
<http://www.net-security.org/conference.php?id=123>

The 4th International Workshop for Applied PKI (IWAP'05)
Organized by Institute for Infocomm Research - 21 September-23 September 2005
<http://www.net-security.org/conference.php?id=124>

IT Security World 2005 Conference & Expo
Organized by MISTI - 26 September-1 October 2005
<http://www.net-security.org/conference.php?id=143>

HealthSec 2005 Conference & Expo
Organized by MISTI - 28 September-30 September 2005
<http://www.net-security.org/conference.php?id=141>

RSA Conference Europe 2005
Organized by RSA Conference - 17 October-19 October 2005
<http://www.net-security.org/conference.php?id=133>

CNIS 2005: IASTED International Conference on Communication, Network and Information Security
Organized by IASTED - 14 November-16 November 2005
<http://www.net-security.org/conference.php?id=137>

Asiacrypt 2005

Organized by International Association for Cryptologic Research - 1
December-4 December 2005

<http://www.net-security.org/conference.php?id=125>

3rd International IEEE Security in Storage Workshop

Organized by IEEE Computer Society - 13 December-13 December 2005

<http://www.net-security.org/conference.php?id=140>

RSA Conference 2006

Organized by RSA Security - 13 February-17 February 2006

<http://www.net-security.org/conference.php?id=142>

[Security World]

All press releases are located at:

http://www.net-security.org/press_main.php

Send your press releases to press@net-security.org

SSH Communications Security Announces Mika Peuranen As Chief
Financial Officer

<http://www.net-security.org/press.php?id=3361>

Sophos Identifies The Most Prevalent Spam Categories Of 2005

<http://www.net-security.org/press.php?id=3360>

Elemental Cto Dan Farmer Recognized As A Technology Visionary By
Infoworld Magazine, Named An "Innovator To Watch In 2006"

<http://www.net-security.org/press.php?id=3359>

HNS Consulting Announces the Release of Confidential Notes 1.1 and
the Nomination for the Pocket PC Magazine Best Software Awards 2005

<http://www.net-security.org/press.php?id=3358>

ICSA Labs certifies the protection capability of Panda ExchangeSecure
Antivirus

<http://www.net-security.org/press.php?id=3357>

Preventsys Expands Into Canada With Cyberklix Partnership
<http://www.net-security.org/press.php?id=3356>

Emental Names Engineering VP, Further Broadens Depth Of Experience Of Security Compliance Management Provider
<http://www.net-security.org/press.php?id=3355>

Pointsec Positioned in Leader Quadrant of Mobile Data Protection Magic Quadrant
<http://www.net-security.org/press.php?id=3354>

GFI MailSecurity 9 serves up premium server-based email security on a silver platter
<http://www.net-security.org/press.php?id=3353>

Results of nCipher "Cryptography in the Enterprise" Survey 2005
<http://www.net-security.org/press.php?id=3352>

CyberGuard Adds Information Security Expert to Manage Growing Middle East Operation
<http://www.net-security.org/press.php?id=3351>

F-Secure first to launch Mobile Anti-Virus for the retail market
<http://www.net-security.org/press.php?id=3350>

MessageLabs and Scansafe Announce Strategic Partnership To Provide Integrated Managed Security For Both Email And Web
<http://www.net-security.org/press.php?id=3349>

Stratecast Partners Grants Senforce 'Best in Class' Award for Constant and Comprehensive Endpoint Security
<http://www.net-security.org/press.php?id=3348>

SmoothWall Consolidates Partner Programme In Bid To Double Reseller Base
<http://www.net-security.org/press.php?id=3347>

[Virus News]

All virus news are located at:
<http://www.net-security.org/viruses.php>

Weekly Report on Viruses and Intruders - Infober.A, Incef.A and
Bobax.AU.
http://www.net-security.org/virus_news.php?id=568

Questions, contributions, comments or ideas go to:

Help Net Security staff
staff@net-security.org
<http://net-security.org>

Unsubscribe from this weekly digest on:
<http://www.net-security.org/subscribe.php>

The archive of the newsletter in TXT and PDF format is available
http://www.net-security.org/newsletter_archive.php

InfoSec Research Library - <http://net-security.bitpipe.com>

In association with BitPipe, Help Net Security is giving you a
possibility to freely read the latest white papers, case studies,
webcasts and product information related to information security.

Some of the topics covered include: Authentication, Email Security,
Identity Management, Network Security, Security Policies. VPN and
Wireless Security.

Point your browsers to: <http://net-security.bitpipe.com>
