

HNS Newsletter  
Issue 297 - 26.12.2005.  
<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.

---

"How A Hacker Launches A Blind SQL Injection Attack Step-by-Step" WP

---

The newest web app vulnerability... Blind SQL Injection!  
Even if your web application does not return error messages, it may still be open to a Blind SQL Injection Attack. Blind SQL Injection can deliver total control of your server to a hacker giving them the ability to read, write and manipulate all data stored in your backend systems! Download this \*FREE\* white paper from SPI Dynamics for a complete guide to protection!

---

Download whitepaper from: <http://www.net-security.org/v/spidyn2>

---

Table of contents:

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

[ Security news ]

---

**INDUSTRY GIVES U.S. SECURITY EFFORTS CS AND DS**  
A group of technology companies released a national agenda for information security this week, rating the current U.S. government's efforts in protecting data and the Internet with a below-average grade.  
<http://www.net-security.org/news.php?id=9768>

**WHY EMAIL COMPLIANCE AND ENCRYPTION CANNOT BE IGNORED**  
This FREE 90-minute educational Webcast features Paul Stamp, Forrester Research's security expert and global authority on messaging security.  
<http://www.net-security.org/news.php?id=9769>

**RESEARCHERS: FLAW AUCTIONS WOULD IMPROVE SECURITY**  
The auction may have set a record price for a highlighter pen and an 8-by-11-inch sheet of paper.  
<http://www.net-security.org/news.php?id=9770>

**VIRUS FIGHTERS CAN'T KEEP UP**

At 5:07 p.m. on Dec. 21 a year ago this week, the Santy worm arrived at Kaspersky Lab in Moscow via an E-mail message.  
<http://www.net-security.org/news.php?id=9771>

**RFID POISED FOR INVESTMENT EXPLOSION**  
Spending expected to skyrocket by 2010.  
<http://www.net-security.org/news.php?id=9772>

**PRESIDENT BUSH, NSA ACCUSED OF WIRETAP ABUSE**  
In an article published in the New York Times, journalists claim that the National Security Agency (NSA) has and continues to engage in covert, extralegal domestic surveillance of American citizens and foreign nationals.  
<http://www.net-security.org/news.php?id=9773>

**OMG PUSHES STANDARDS FOR VERIFYING SOFTWARE SECURITY**  
A report released early this month by a task force within the Object Management Group outlines the standards needed to develop a consistent process for verifying the security of software sold to government agencies.  
<http://www.net-security.org/news.php?id=9774>

**IT SECURITY PROFESSIONALS MOVE ON UP**  
Information security professionals are now more highly regarded, and are moving up the corporate ladder towards the board, according to a survey by analyst firm IDC.  
<http://www.net-security.org/news.php?id=9775>

**HOLES FOUND IN PC VIRUS DEFENCES**  
People using Windows computers were unprotected against new viruses for 56 days this year, research shows.  
<http://www.net-security.org/news.php?id=9776>

**WINDOWS MOBILE 2005 SECURITY MODEL FAQ**  
Here are some questions and answers that will point you in the right direction.  
<http://www.net-security.org/news.php?id=9777>

**DASHER WORM INFECTS 3,000 MACHINES**  
Dasher worm infects 3,000 machines  
<http://www.net-security.org/news.php?id=9778>

**TIPS ON HOW TO BEAT ONLINE FRAUDSTERS**  
Organized criminal gangs are targeting online consumers with ever more sophisticated blended phishing attacks, some of which even find out details of their interests and use them to generate phishing emails tailored to tempt them into giving away their identities.  
<http://www.net-security.org/news.php?id=9779>

**UPDATE GLITCH SPINS OUT IE7 BETA TESTERS**  
Last week's update for Internet Explorer has tripped up users testing

an early pre-release version of IE7.  
<http://www.net-security.org/news.php?id=9780>

**SECURITY-ENHANCED LINUX MOVING INTO MAINSTREAM**  
SELinux provides mandatory access control to a wider audience. It helps eliminate O-day attacks.

<http://www.net-security.org/news.php?id=9781>

**THE WORST NETWORK SECURITY HORROR STORIES**  
Think you've had security problems? You aint heard nothing yet. We asked the pros to tell us some of the worst disasters they've faced. Here's what they told us.  
<http://www.net-security.org/news.php?id=9782>

**SOCIAL ENGINEERING AND OTHER THREATS TO INTERNAL SECURITY**  
How does a company protect itself from its own users who intentionally or accidentally can cause serious damage?  
<http://www.net-security.org/news.php?id=9783>

**BEST PRACTICES FOR SECURITY ROUTING PROTOCOLS**  
This document discusses the various threats against routing protocols, including peering disruption and falsifying of routing information, followed by a description of the methods and techniques used to attack a routing system.  
<http://www.net-security.org/news.php?id=9784>

**SECURITY EXPERTS URGE A 'SAY YES' MINDSET**  
Being an IT security specialist requires a close understanding of business goals, a dose of salesmanship and a willingness to say yes to projects even if it means dealing with new risks, top network security professionals told attendees at last week's inaugural Interop New York.  
<http://www.net-security.org/news.php?id=9785>

**UK SHELTERS FROM SMUT TROJAN BLITZ**  
UK businesses were targeted in a blitz of 215,000 emails containing a new Trojan on Monday (19 December), according to email filtering firm BlackSpider Technologies. The malware - called Small-BXP - comes in the payload to a message that poses as a receipt for access to an online porn site.  
<http://www.net-security.org/news.php?id=9786>

**SECURING CARD DATA ISN'T AN EASY SELL**  
Recent data compromises, such as one involving the Sam's Club wholesale chain, highlight the challenges that credit card companies face in enforcing the security standards that went into effect last July for all businesses processing credit transactions.  
<http://www.net-security.org/news.php?id=9787>

**ENCRYPTING WITHOUT SECRETS**  
Do you have a Web site or other system that deals in secrets of any

sort? It seems like every time I give a security talk, people ask how to deal with the sticky problem of storing secrets.  
<http://www.net-security.org/news.php?id=9788>

#### NUMBER OF VIRUS THREATS CONTINUES TO RISE

Medical-related spam, which claims to assist in sexual performance or weight loss, will remain the most dominant type of spam next year, said Sophos managing director Charles Cousins.  
<http://www.net-security.org/news.php?id=9789>

#### USE OF WI-FI UP BUT CONCERNS OVER HOTSPOT COST AND SECURITY REMAIN

Sales of Wi-Fi-enabled devices have increased 64% this year and will exceed 120 million units before the year is out, according to research firm In-Stat. But analysts said many organisations are still wary of the technology.  
<http://www.net-security.org/news.php?id=9790>

#### TERROR PHONE CLONE SCAM EXPOSED

Affiliates of terrorist organization Hezbollah cloned the mobiles of senior executives of Canadian operator Rogers Communications, including chief exec Ted Rogers.  
<http://www.net-security.org/news.php?id=9791>

#### OPENSSEH CUTTING EDGE

Federico Biancuzzi interviews OpenSSH developer Damien Miller to discuss features included in the upcoming version 4.3, public key crypto protocols details, timing based attacks and anti-worm measures.  
<http://www.net-security.org/news.php?id=9792>

#### MERGERS, SECURITY SHAPED NETWORKING YEAR

There wasn't a moment's peace in the world of networking in 2005, from big carrier mergers announced early in the year, through a security bombshell and some major high-speed wireless launches.  
<http://www.net-security.org/news.php?id=9793>

#### MICROSOFT RELEASES SECURITY FOCUSED VISTA PREVIEW

December CTP offers security, portability and performance enhancements.  
<http://www.net-security.org/news.php?id=9794>

#### CHILE AND PERU FIGHT MERCILESS HACKER WAR

Official websites hit as fish crisis escalates.  
<http://www.net-security.org/news.php?id=9795>

#### SELLING PEOPLE INFORMATION ABOUT THEMSELVES

The online security of a popular game maker was compromised last week, with hackers demanding an undisclosed sum to prevent data exposure. White Wolf Publishing posted a statement on their website indicating they had no intent of paying the hackers.  
<http://www.net-security.org/news.php?id=9796>

**ORACLE FORTIFIES APPLICATION SECURITY AT THE SOURCE**  
Oracle had previously relied on source-code analysis tools developed in-house but decided to work with a third party.  
<http://www.net-security.org/news.php?id=9797>

**MOBILE SECURITY THREATS TO RISE IN 2006**  
martphone users beware - mobile malware is set to triple in the coming year, according to security experts.  
<http://www.net-security.org/news.php?id=9798>

**OPEN SOURCE APPLICATION SCHOOL: SECURITY ADMINISTRATION TOOLS**  
Find out about Snort and other enterprise-ready open source security applications in this Webcast. Expert speaker Bernard Golden offers a guide to choosing and using security management and administration applications.  
<http://www.net-security.org/news.php?id=9799>

**AUTHENTICATION ANGST**  
Minor glitches dog vendor implementations of RADIUS and LDAP-based authentication ties.  
<http://www.net-security.org/news.php?id=9800>

**SOBER WORM PROMPTS NET PERV CONFESSION**  
A child porn suspect turned himself in to the police after mistaking an email generated by a prolific internet worm for an official notice he was under investigation.  
<http://www.net-security.org/news.php?id=9801>

**COMPUTER FORENSICS FIRM GUIDANCE HACKED**  
Computer forensics firm Guidance Software has itself become the subject of a hack attack, prompting warnings to its clients in law enforcement and computer security that their financial details may have been exposed.  
<http://www.net-security.org/news.php?id=9802>

**BUILDING THE PERFECT SSL VPN**  
Picking and choosing features from among the top tested products.  
<http://www.net-security.org/news.php?id=9803>

**ROOTKIT GURU: ANTIVIRUS MAKES ME DO IT**  
Smart computer users know that once a computer is infected by a rootkit, it's changed forever. And as Windows rootkits go, Hacker Defender is among the most dangerous. The author of Hacker Defender, holy\_father, explains why he does what he does, and what you can do to detect his rootkit.  
<http://www.net-security.org/news.php?id=9804>

**FTC: COMPUTER USERS SEEING LESS SPAM**  
Agency cites CAN-SPAM Act as reason for reduction in unsolicited e-mail.  
<http://www.net-security.org/news.php?id=9805>

#### ORACLE TURNS TO FORTIFY TO SECURE SOURCE CODE

Oracle to use startups tools to find problems in database and middleware.

<http://www.net-security.org/news.php?id=9806>

#### SECURITY: FORENSIC TOOLS IN COURT

An interesting question comes to mind when you use as many open source forensic and security tools as I do — if I ever go to court over this case, will my tools be considered valid?

<http://www.net-security.org/news.php?id=9807>

#### SUNBELT COMPLETES KERIO FIREWALL BUY

Sunbelt Software on Tuesday completed its acquisition of Kerio's desktop and server firewall products, a move which will save the popular free Kerio Personal Firewall from its planned retirement. In addition, Sunbelt is lowering the price of the full version to \$19.95.

<http://www.net-security.org/news.php?id=9808>

#### SANTA WORM ON MSN, AOL, ICQ, & YAHOO PLANTS ROOTKIT

A new worm posing as a come-on to a Santa Claus site is traveling across all the major instant messaging networks, a security firm warned Tuesday, and when recipients visit the bogus site, they're infected with a file hidden from sight by a rootkit.

<http://www.net-security.org/news.php?id=9809>

#### US 'WINNING WAR' ON E-MAIL SPAM

The number of unsolicited e-mails received in the US appears to be falling thanks to new laws and better technology, a government report says.

<http://www.net-security.org/news.php?id=9810>

#### LOOKING BACK AT COMPUTER SECURITY IN 2005

This article presents a view on some of the biggest events of 2005 with comments by Bruce Schneier, Howard Schmidt, Dr. Gerhard Eschelbeck, Mikko H. Hyppönen, Ira Winkler and Fyodor.

<http://www.net-security.org/news.php?id=9811>

#### EU DATA TO BE STORED FOR TWO YEARS

European telecoms companies and ISPs will have to keep their data stored for two years to meet security regulations after EU politicians and legislators voted for the increase in data retention.

<http://www.net-security.org/news.php?id=9812>

#### HI-TECH SECURITY SYSTEMS TESTED ON LONDON RAIL

Body Imaging scanners or sophisticated CCTV which can automatically spot suspicious behaviour could be introduced on parts of the rail and Tube networks to combat the threat of suicide terrorists.

<http://www.net-security.org/news.php?id=9813>

#### CHOOSING THE RIGHT EAP TYPE FOR WIRELESS LAN SECURITY

To ensure the security of a WLAN, its connection with wireless client devices must be authenticated and encrypted, this is accomplished via encryption protocols such as WPA, WPA2 and WEP in addition to the 802.1x authentication protocol.

<http://www.net-security.org/news.php?id=9814>

#### QUANTUM CRYPTOGRAPHY: WHEN YOUR LINK HAS TO BE REALLY SECURE

QC (quantum cryptography) uses a string of individual photons and their quantum states as the bases of a link in which physicist Werner Heisenberg's often-cited, often-misunderstood uncertainty principle defeats any eavesdropper.

<http://www.net-security.org/news.php?id=9815>

#### NUMBER OF VIRUS THREATS CONTINUES TO RISE

Medical-related spam, which claims to assist in sexual performance or weight loss, will remain the most dominant type of spam next year, said Sophos managing director Charles Cousins. Other categories of spam expected to rise next year are stock-related spam and pitches for adult content.

<http://www.net-security.org/news.php?id=9816>

#### SERIOUS FLAW REPORTED IN SYMANTEC ANTIVIRUS SOFTWARE

Attackers could gain control of systems by using heap overflows.

<http://www.net-security.org/news.php?id=9817>

#### NESSUS 3.0: THE END OF THE AGE OF OPEN-SOURCE INNOCENCE?

"Here's the danger we are running into," said Alan Shimmel, Chief Strategy Officer for StillSecure. "People contribute resources to these communities, whether it be time, money, or code. When they see everything they give converted for the commercial success of an individual rather than as a community as a whole, how long do you think they are going to want to keep giving?"

<http://www.net-security.org/news.php?id=9818>

#### FORD COMPUTER WITH EMPLOYEE DATA STOLEN

The data includes Social Security numbers; a letter has been sent to employees urging them to take steps to safeguard their personal information.

<http://www.net-security.org/news.php?id=9819>

#### HOW TO MANAGE SECURITY HALFWAY AROUND THE WORLD

Different cultures. Unstable political environments. Language barriers. CSOs in global companies face many a challenge as they try to manage security in far-flung locations. One of the biggest challenges?

<http://www.net-security.org/news.php?id=9820>

#### REAL WORLD SECURITY THREATS: THE ANATOMY OF A HACK

In this on-demand video demonstration and companion guide, watch as a hacker takes complete control of a mobile endpoint system without the proper security protection, and is able to attack and gain access to the mobile endpoint.

<http://www.net-security.org/news.php?id=9821>

#### FOUR SECURITY RESOLUTIONS FOR THE NEW YEAR

I always know what my first New Year's resolution is going to be, because it's the same every year: lose weight. Chances are, you have the same one. But by the time the Super Bowl happens, and you eat seven thousand calories on that one day, you'll have already have given up on that resolution.

<http://www.net-security.org/news.php?id=9822>

#### TRACKED BY CELLPHONE

We know that technology can be used to track people's location via a cellphone, but how difficult is it for law enforcement to get a court order and do this legally?

<http://www.net-security.org/news.php?id=9823>

#### GOOGLE PLUGS SECURITY HOLES IN WEB SITE

Flaws would have exposed users to phishing scams.

<http://www.net-security.org/news.php?id=9824>

#### ENCRYPTION: A NICE IDEA THAT FEW WANT TO IMPLEMENT?

Companies are not embracing encryption as a way to protect sensitive data. According to Ponemon Institute's 2005 National Encryption Survey, only 4.2% of companies responding to our survey say their organizations have an enterprisewide encryption plan.

<http://www.net-security.org/news.php?id=9825>

#### SECURITY CHECKS IN

N airport security "checkpoint of the future" that lets travellers leave shoes on feet, keys in pockets and laptop computers in carry-on bags has been shown off in San Francisco.

<http://www.net-security.org/news.php?id=9826>

#### TOP 7 PHP SECURITY BLUNDERS

This article details many of the common PHP programming mistakes that can result in security holes.

<http://www.net-security.org/news.php?id=9827>

#### DATA SECURITY MOVEMENT BACKBURNED BY LAWMAKERS

Despite a year's worth of highly publicized security breaches and a lot of talk in Congress this summer on ways to protect consumers, there's been too little done to protect U.S. consumers' data, said Gartner research director Avivah Litan.

<http://www.net-security.org/news.php?id=9828>

-----  
[ Vulnerabilities ]

All vulnerabilities are located here:  
<http://www.net-security.org/vulnerabilities.php>

-----  
AltraSoft EPay Enterprise profile.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21883>

AltraSoft EPay Enterprise card.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21884>

AltraSoft EPay Enterprise bank.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21885>

AltraSoft EPay Enterprise subscriptions.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21886>

AltraSoft EPay Enterprise send.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21887>

AltraSoft EPay Enterprise request.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21888>

AltraSoft EPay Enterprise forgot.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21889>

AltraSoft EPay Enterprise escrow.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21890>

AltraSoft EPay Enterprise donations.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21891>

AltraSoft EPay Enterprise products.htm Unspecified XSS  
<http://www.net-security.org/vulnerability.php?id=21892>

PortalApp login.asp ret\_page Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21880>

Alkacon OpenCms Search Module XSS  
<http://www.net-security.org/vulnerability.php?id=21877>

Slashcode search.pl topic Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21874>

Slashcode submit.pl filter Variable XSS

<http://www.net-security.org/vulnerability.php?id=21875>

e-publish CMS printer\_friendly.cfm id Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21881>

e-publish CMS show.cfm Multiple Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21882>

Lighthouse CMS index.php search Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21852>

Mercury CMS index.cfm page Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21862>

Mercury CMS index.cfm Multiple Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21863>

Direct News index.php setLang Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21854>

Cofax search.htm searchstring Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21850>

ContentServ index.php StoryID variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21851>

WANDSOFT e-SEARCH keywords Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21867>

SyntaxCMS /search/results.php search\_query Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21859>

Tangora Portal CMS action Variable Multiple Page XSS  
<http://www.net-security.org/vulnerability.php?id=21860>

OpenEdit results.html Multiple Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21866>

phpSlash article.php story\_id Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21873>

Community Enterprise index.cfm Multiple Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21855>

Papoo index.php menuid Variable SQL Injection

<http://www.net-security.org/vulnerability.php?id=21869>

Papoo guestbook.php menuid Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21870>

Papoo print.php Multiple Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21871>

SiteEnable login.asp ret\_page Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21879>

Miraserver index.php page Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21836>

Miraserver newsitem.php id Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21837>

Miraserver article.php cat Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21838>

Honeycomb Archive CategoryResults.cfm Multiple Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21827>

Honeycomb Archive search.cfm keyword Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21828>

pTools index.asp docID Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21841>

CONTENS search.cfm near Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21824>

NQcontent Search Module XSS  
<http://www.net-security.org/vulnerability.php?id=21829>

Pegasus Mail POP3 Trace Reply Overflow  
<http://www.net-security.org/vulnerability.php?id=21842>

Pegasus Mail RFC2822 Message Display Overflow  
<http://www.net-security.org/vulnerability.php?id=21843>

Marwel index.php show Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21831>

lemoon Search Module q Variable XSS

<http://www.net-security.org/vulnerability.php?id=21820>

Libertas ECMS /search/index.php page\_search Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21819>

damoon Search Module q Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21817>

iHTML Merchant Mall browse.ihtml Multiple Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21830>

Media2 CMS Shop default.asp item Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21846>

iCMS /admin/Default.asp LoginMSG Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21809>

iCMS RunScript.asp Event\_ID Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21810>

iHTML Merchant Pro merchant.ihtml Multiple Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21808>

Acidcat CMS default.asp ID Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21845>

Template Markup Language (TML) index.php form Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21801>

Template Markup Language (TML) index.php id Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21802>

paFileDB Extreme Edition pafiledb.php Multiple Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21822>

ODFaq faq.php Multiple Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21790>

Free Lanparty Inter-/Intranet Portal (FLIP) text.php name Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21788>

Free Lanparty Inter-/Intranet Portal (FLIP) forum.php frame Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21789>

Komodo CMS page.php page Variable SQL Injection  
<http://www.net-security.org/vulnerability.php?id=21792>

Magnolia Search Feature search.html query Variable XSS  
<http://www.net-security.org/vulnerability.php?id=21795>

Microsoft IIS Crafted URL Remote DoS  
<http://www.net-security.org/vulnerability.php?id=21805>

Imoel CMS setting.php SQL Authentication Credential Cleartext  
Disclosure  
<http://www.net-security.org/vulnerability.php?id=21766>

-----

[ Advisories ]

All advisories are located at:  
[http://www.net-security.org/archive\\_adv.php](http://www.net-security.org/archive_adv.php)

-----

Debian Security Advisory - ketm (DSA 926-2)  
<http://www.net-security.org/advisory.php?id=5750>

Debian Security Advisory - ketm (DSA 926-1)  
<http://www.net-security.org/advisory.php?id=5749>

Ubuntu Security Notice - php4, php5 vulnerabilities (USN-232-1)  
<http://www.net-security.org/advisory.php?id=5748>

Ubuntu Security Notice - linux-source-2.6.8.1/-2.6.10/-2.6.12  
vulnerabilities (USN-231-1)  
<http://www.net-security.org/advisory.php?id=5747>

SCO Security Advisory - OpenServer 6.0.0 : TCP Denial of Service  
Vulnerability (SCOSA-2005.65)  
<http://www.net-security.org/advisory.php?id=5746>

SCO Security Advisory - UnixWare 7.1.3 UnixWare 7.1.4 : TCP Denial of  
Service Vulnerability (SCOSA-2005.64)  
<http://www.net-security.org/advisory.php?id=5745>

Conectiva Linux Security Announcement - lynx regression fix  
(CLA-2005:1053)

<http://www.net-security.org/advisory.php?id=5744>

Conectiva Linux Security Announcement - libungif4 vulnerabilities  
(CLA-2005:1052)

<http://www.net-security.org/advisory.php?id=5743>

Conectiva Linux Security Announcement - graphviz (CLA-2005:1051)

<http://www.net-security.org/advisory.php?id=5742>

Debian Security Advisory - phpbb2 (DSA 925-1)

<http://www.net-security.org/advisory.php?id=5741>

Mandriva Linux Security Update Advisory - kernel (MDKSA-2005:235)

<http://www.net-security.org/advisory.php?id=5740>

Debian Security Advisory - nbd (DSA 924-1)

<http://www.net-security.org/advisory.php?id=5739>

SCO Security Advisory - OpenServer 5.0.6 OpenServer 5.0.7 OpenServer  
6.0.0 : wu-ftp Denial of Service Vulnerability (SCOSA-2005.63)

<http://www.net-security.org/advisory.php?id=5738>

HP Security Bulletin - HP-UX running WBEM Services Denial of Service  
(DoS) (HPSBMA02088 SSRT051026 rev. 1)

<http://www.net-security.org/advisory.php?id=5737>

HP Security Bulletin - HP-UX Running Software Distributor (SD)  
Remote Unauthorized Access (HPSBUX02089 SSRT5983 rev.1)

<http://www.net-security.org/advisory.php?id=5736>

Mandriva Linux Security Update Advisory - sudo (MDKSA-2005:234)

<http://www.net-security.org/advisory.php?id=5735>

SCO Security Advisory - OpenServer 5.0.6 OpenServer 5.0.7 OpenServer  
6.0.0 : Xloadimage NIFF Image Title Handling Buffer Overflow  
Vulnerability (SCOSA-2005.62)

<http://www.net-security.org/advisory.php?id=5734>

SUSE Security Announcement - perl (SUSE-SA:2005:071)

<http://www.net-security.org/advisory.php?id=5733>

SUSE Security Announcement - ipsec-tools, freeswan, openswan  
(SUSE-SA:2005:070)

<http://www.net-security.org/advisory.php?id=5732>

Mandriva Linux Security Update Advisory - apache2 (MDKSA-2005:233)

<http://www.net-security.org/advisory.php?id=5731>

Debian Security Advisory - dropbear (DSA 923-1)  
<http://www.net-security.org/advisory.php?id=5730>

Fedora Legacy Update Advisory - Updated util-linux and mount packages  
fix security issue (FLSA:168326)  
<http://www.net-security.org/advisory.php?id=5729>

Fedora Legacy Update Advisory - Updated openssl packages fix security  
issues (FLSA:166939)  
<http://www.net-security.org/advisory.php?id=5728>

Fedora Legacy Update Advisory - Updated gtk2 packages fixes security  
issues (FLSA:155510)  
<http://www.net-security.org/advisory.php?id=5727>

Fedora Legacy Update Advisory - Updated encript package fixes  
security issues (FLSA:152892)  
<http://www.net-security.org/advisory.php?id=5726>

Fedora Legacy Update Advisory - Updated a2ps package fixes security  
issue (FLSA:152870)  
<http://www.net-security.org/advisory.php?id=5725>

Fedora Legacy Update Advisory - Updated lynx package fixes security  
issues (FLSA:152832)  
<http://www.net-security.org/advisory.php?id=5724>

Fedora Update Notification - Updated redhat-config-nfs package fixes  
security issue (FLSA:152787)  
<http://www.net-security.org/advisory.php?id=5723>

Ubuntu Security Notice - ffmpeg vulnerability (USN-230-1)  
<http://www.net-security.org/advisory.php?id=5722>

Ubuntu Security Notice - xine-lib vulnerability (CVE-2005-4048)  
<http://www.net-security.org/advisory.php?id=5721>

-----

[ Articles ]

All articles are located at:  
[http://www.net-security.org/articles\\_main.php](http://www.net-security.org/articles_main.php)

Articles can be contributed to [articles@net-security.org](mailto:articles@net-security.org)

---

#### LOOKING BACK AT COMPUTER SECURITY IN 2005

This article presents a view on some of the biggest events of 2005 with comments by Bruce Schneier, Howard Schmidt, Dr. Gerhard Eschelbeck, Mikko H. Hyppönen, Ira Winkler and Fyodor.

<http://www.net-security.org/article.php?id=883>

---

#### SOCIAL ENGINEERING AND OTHER THREATS TO INTERNAL SECURITY

How does a company protect itself from its own users who intentionally or accidentally can cause serious damage?

<http://www.net-security.org/article.php?id=882>

---

#### [ Software ]

Windows software is located at:

[http://net-security.org/software\\_main.php?cat=1](http://net-security.org/software_main.php?cat=1)

Linux software is located at:

[http://net-security.org/software\\_main.php?cat=2](http://net-security.org/software_main.php?cat=2)

Pocket PC software is located at:

[http://net-security.org/software\\_main.php?cat=3](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](http://net-security.org/software_main.php?cat=5)

---

#### BOTAN 1.4.10 (Linux)

Botan aims to be a portable, easy to use, and efficient C++ crypto library.

<http://www.net-security.org/software.php?id=94>

#### DANSGUARDIAN 2.9.3.1 (Linux)

DansGuardian is a web content filter. It filters the actual content of pages based on many methods including phrase matching, PICS filtering and URL filtering.

<http://www.net-security.org/software.php?id=233>

#### DEVICELOCK 5.73 (Windows)

DeviceLock gives network administrators control over which users can access what devices on a local computer.

<http://www.net-security.org/software.php?id=121>

#### DISTRIBUTED ACCESS CONTROL SYSTEM 1.4.9 (Linux)

DACS is an open source identity management and access control system

for web services.

<http://www.net-security.org/software.php?id=346>

DROPBEAR SSH SERVER 0.47 (Linux)

Dropbear is an SSH 2 server, designed to be usable in small memory environments.

<http://www.net-security.org/software.php?id=490>

JOHN THE RIPPER 1.6.40 (Linux)

John the Ripper is a fast password cracker.

<http://www.net-security.org/software.php?id=11>

LINUX-VSERVER 2.1.0 (Linux)

A system for running general purpose virtual servers on one box at full speed.

<http://www.net-security.org/software.php?id=527>

MARADNS 1.2.00 (Linux)

MaraDNS is a DNS server that strives to be secure and fully open-sourced.

<http://www.net-security.org/software.php?id=84>

PORTSLOCK 1.8 (Windows)

PortsLock is a personal firewall for Windows NT/2000/XP that fully supports user-level security.

<http://www.net-security.org/software.php?id=120>

RSSH 2.3.0 (Linux)

rssh is a restricted shell for use with OpenSSH, allowing only scp and/or sftp.

<http://www.net-security.org/software.php?id=236>

SAMHAIN 2.1.1a (Linux)

Samhain is an open source file integrity and host-based intrusion detection system.

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

SCPONLY 4.2 (Linux)

"scponly" is an alternative 'shell' (of sorts) for system administrators who would like to provide access to remote users to both read and write local files without providing any remote execution privileges.

<http://www.net-security.org/software.php?id=337>

VISUALROUTE 2006 10.0e (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>

WINSCP 3.8 beta (Windows)

WinSCP is an open source SSH file transfer protocol and secure copy client for Windows using SSH.

<http://www.net-security.org/software.php?id=6>

XYRIA:DNSD 0.7.1 (Linux)

Xyria:DNSd is a high performance DNS server that supports only the most important features and resource records while being extremely fast and secure.

<http://www.net-security.org/software.php?id=93>

-----

[ Conferences ]

All conferences are located at:

<http://net-security.org/conferences.php>

-----

Black Hat Federal 2006 Briefings and Training

Organized by Black Hat - 23 January-26 January 2006

<http://www.net-security.org/conference.php?id=150>

RSA Conference 2006

Organized by RSA Security - 13 February-17 February 2006

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

Black Hat Europe 2006 Briefings and Training

Organized by Black Hat - 28 February-3 March 2006

<http://www.net-security.org/conference.php?id=151>

LayerOne 200

Organized by LayerOne - 22 April-23 April 2006

<http://www.net-security.org/conference.php?id=154>

iTrust 2006

Organized by IIT-CNR - 16 May-19 May 2006

<http://www.net-security.org/conference.php?id=152>

Eurocrypt 2006

Organized by IACR - 28 May-1 June 2006

<http://www.net-security.org/conference.php?id=153>

-----

[ Security World ]

All press releases are located at:  
[http://www.net-security.org/press\\_main.php](http://www.net-security.org/press_main.php)

Send your press releases to [press@net-security.org](mailto:press@net-security.org)

---

AEP Netilla Security Platform Achieves High Marks in Network World's  
SSL VPN Interoperability Testing  
<http://www.net-security.org/press.php?id=3722>

New Uimix Software Hides Sensitive Information from Prying Eyes  
<http://www.net-security.org/press.php?id=3721>

Santa Claus leaves you a Trojan for Christmas  
<http://www.net-security.org/press.php?id=3720>

MacScan, Long Awaited Spyware Protection Software, Released for Mac  
OS X  
<http://www.net-security.org/press.php?id=3719>

SSH Signs Multi-Year Agreements With Three Major Enterprises  
<http://www.net-security.org/press.php?id=3718>

Panda GateDefender 8200 awarded NSS Approved certification  
<http://www.net-security.org/press.php?id=3717>

Elemental Security Compliance Management Product Honored By Editors  
Of Info Security Products Guide  
<http://www.net-security.org/press.php?id=3716>

HoneyNet - Getting back to basics  
<http://www.net-security.org/press.php?id=3715>

O'Reilly Releases "Internet Forensics"  
<http://www.net-security.org/press.php?id=3714>

Electronic Christmas gifts a risk factor for companies  
<http://www.net-security.org/press.php?id=3713>

---

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](http://www.net-security.org/newsletter_archive.php)